Gedeelde en samengestelde identiteiten in de publieke dienstverlening

van der Hof, S.; Leenes, R.E.

Publication date:
2010

Document Version
Peer reviewed version

Gedeelde en samengestelde identiteiten in de publieke dienstverlening

dr. Simone van der Hof, Universiteit van Tilburg
prof.dr. Ronald Leenes, Universiteit van Tilburg

Tilburg, april 2010

Inhoud

1. Inleiding en probleemstelling 5

1.1 Onderzoeksdoel en -vragen 6

1.2 Methodologie 6

1.3 Plan 7

2. Identiteit 9

2.1 Inleiding 9

2.2 Historische ontwikkeling 10

2.3 Conclusie 15

3. Digitale identiteiten 17

3.1 Inleiding 17

3.2 Van record naar digitale identiteit 18

3.3 Digitale identiteit komt tot leven 22

3.4 Een eigen leven 24

3.5 Conclusie 26

4. Samengestelde en gedeelde identiteiten 27

4.1 Inleiding 27

4.2 Van enkelvoudige naar samengestelde identiteiten 27

4.3 Van samengestelde naar gedeelde identiteiten 30

4.4 Van beleidskokers naar maatschappelijke ketens 31

4.5 Focus op risico's, veiligheid en preventie 32

4.6 De schaduwkant van moderne identiteiten 34

4.7 Conclusie 42

5. Praktijkvoorbeeld: het EKD **45**

5.1 Inleiding ***45***

5.2 Het EKD: Van enkelvoudige naar gedeelde identiteiten ***46***

5.3 Conclusie ***48***

6. Conclusies **49**

6.1 Trends en definities ***49***

6.2 Risico's ***51***

6.3 Slotoverwegingen ***53***

Bibliografie **56**

Bijlagen **59**

1. Inleiding en probleemstelling

De publieke en private dienstverlening aan burgers en klanten vindt toenemend plaats via elektronische netwerken. Elektronische dossiers vormen hier digitale representaties van relevante aspecten van de identiteit van betrokkenen. Dergelijke ‘digital personae’ (Clarke, 1994) zijn toegankelijk via ‘identifiers’ zoals naam en adres, en het BurgerServiceNummer in de publieke sector. Nieuwe wijzen van identificatie en authenticatie van de burger, zoals BSN, biometrische paspoort en DIGID, moeten de uitwisseling van digital personae in de publieke sector vereenvoudigen en verbeteren, terwijl een roep vanuit de private sector bestaat om gebruik te mogen maken van publieke ‘identifiers’, zoals BSN.

Van ieder individu bestaan vele (digitale) deel-identiteiten die tezamen haar 'volledige' digitale identiteit bestrijken. We zijn moeder, wetenschapper, amateur tennisser, politiek activiste en belastingbetaler tegelijkertijd. De gezichten die we van onszelf laten zien in de diverse rollen verschillen. Vanuit sociologisch perspectief is het kunnen onderscheiden van deel-identiteiten noodzakelijk (Goffman, 1956). Intimiteit, sociale rollen, ontplooiing, en eigenlijk sociaal functioneren, is afhankelijk van de scheiding van verschillende sociale contexten en de bijbehorende informatie (Introna, 1997, p. 265, Rachels, 1975).

Vanuit het perspectief van gebruikers van elektronische dossiers lijkt het bestaan van een bonte verzameling van verschillende ‘digital personae’ binnen publieke en private sector inefficiënt en ineffectief en er is dan ook een roep om gegevensverzamelingen te koppelen, of op z'n minst de toegang tot de verschillende bij een individu behorende identiteiten te vergemakkelijken. Dat levert echter ook risico's op. Veelvuldig is gewezen op de gevaren van misbruik van persoonsgegevens bij het gebruik van uniforme ‘identifiers’, zoals het BSN (vgl. Grijpink, 2006, Prins en Meulen, 2006), en het “openstellen” van de publieke sector zou deze gevaren nog verder vergroten, omdat dit de personenkring met toegang tot de ‘identifiers’ nog verder vergroot.

De invloed van koppeling en het gebruik van uniforme ‘identifiers’ op onze (digitale) identiteit is een meer fundamentele vraag die nog onderbelicht is. Verschillende auteurs stellen dat het samenvoegen en toegankelijk maken van digitale identiteiten buiten de contexten waarin deze zijn gecreëerd risico's oplevert met betrekking tot de interpretatie van de resultaten doordat noodzakelijke context-informatie ontbreekt of de samengestelde digitale identiteiten inconsistente of onjuiste representaties van de betrokken opleveren (zie bijv. Clarke, 1994, p. 13, Gandy, 1993, Lyon, 2001, pp 21-27, 2004, pp 142-143, Solove, 2007a, p. 66). Bovendien komt onze sociale identiteit onder druk doordat koppeling en uitwisseling van digitale identiteiten onze mogelijkheden sociale contexten te scheiden verkleint (Introna, 1997).

1.1 Onderzoeksdoel en -vragen

In het algemeen beoogt het onderzoek bij te dragen aan de begripsvorming omtrent de sociale effecten van het inter-contextuele gebruik van digitale identiteiten op het individu.

Meer specifiek is het **doel** van dit onderzoek om in kaart te brengen hoe samengestelde of gedeelde digitale identiteiten in de publieke sector contexten worden geconstrueerd en wat de potentiële effecten daarvan zijn voor de burger en de gebruikers van digitale identiteiten in de publieke sector. Daarbij wordt zowel gekeken naar informatie die het individu zelf beschikbaar stelt ('projected digital personae') als naar waarnemingen (en oordelen) door de publieke entiteiten als onderdeel van de geconstrueerde digitale identiteiten ('imposed digital personae').

De **centrale vraagstelling** van het onderzoek is: *wat zijn de mogelijke consequenties van het gebruik van gedeelde en samengestelde identiteiten voor gebruikers en voor burgers, gelet op de wijze waarop dergelijke identiteiten in de publieke sector worden gevormd en toegepast?*

De centrale vraagstelling wordt verder onderverdeeld in de volgende **subvragen**:

- Hoe kunnen samenstelde en gedeelde (digitale) identiteiten worden gedefinieerd?
- Hoe worden samengestelde en gedeelde identiteiten in de publieke sector gevormd en toegepast?
- Wat zijn (potentiële) risico's aan de constructie en het gebruik van samengestelde en gedeelde identiteiten?

1.2 Methodologie

Aan de hand van literatuurstudie wordt een theoretisch kader neergezet. Bij de ontwikkeling van het theoretisch kader is aangesloten bij reeds lopend onderzoek binnen TILT (PRIME, FIDIS en NWO/NVN-project 'Framing Citizen's Identities'). Een belangrijk uitgangspunt in het theoretisch kader vormt werk van Irving Goffman. Ofschoon Goffman zich voornamelijk richtte op face-to-face interacties tussen individuen, kan inmiddels worden aangenomen dat zijn ideeën mede kunnen worden doorgetrokken naar de digitale omgeving (zie onder meer Robinson, 2007).

Verder is een case study uitgevoerd waarbij is onderzocht om welke redenen en op welke wijze gedeelde identiteiten worden geconstrueerd in de publieke sector. De case study betreft het elektronisch kind dossier (EKD). De casestudy is uitgevoerd aan de hand van persoonlijke interviews met de bij de casus betrokken sleutelpersonen op strategisch, beleids- en operationeel niveau en op basis van beleidsdocumenten.

1.3 Plan

In hoofdstuk 2 wordt kort de geschiedenis van het begrip ‘identiteit’ beschreven om enig inzicht te geven in de betekenissen en complexiteit van dit concept. Hoofdstuk 3 analyseert het concept ‘digitale identiteiten’ en laat zien hoe deze identiteiten zich in de moderne samenleving ontwikkelen tot digitale representaties van burgers. In hoofdstuk 4 wordt uitgewerkt hoe en wanneer digitale identiteiten samengestelde en gedeelde identiteiten kunnen worden alsmede wat op fundamenteel en praktisch niveau potentiële risico’s zijn aan het gebruik van dergelijke moderne digitale identiteiten. Hoofdstuk 5 licht aan de hand van het Elektronisch Kind Dossier het ontstaan van samengestelde en gedeelde identiteiten in de praktijk toe. Met conclusies in hoofdstuk 6 wordt het rapport afgesloten.

2. Identiteit

2.1 Inleiding

Binnen de publieke sector wordt op grote schaal gebruik gemaakt van elektronische netwerken en databestanden in de uitvoering van publieke taken. De databestanden bevatten informatie over individuele burgers in hun gedaante als staatsburger, onderdaan, kiezer en klant (Ringeling, 2001). Teneinde de efficiëntie van het overheidshandelen te vergroten, fouten te verminderen en burgers minder onnodig lastig te vallen wordt in toenemende mate gewerkt met authentieke registraties waarin gecontroleerde en juiste basisinformatie staat over de burger. Het gebruik van basisregistraties impliceert de uitwisseling van gegevens over betrokkenen in het uitvoeringsproces. Ook op andere plaatsen zien we een koppeling van gegevensbestanden teneinde processen te stroomlijnen en verbeteren.

Het gebruik en de uitwisseling van gegevens over burgers raakt aan het thema privacy en dataprotectie. Gegevens over burgers zijn namelijk vrijwel altijd persoonsgegevens in de zin van artikel 2 van de Wet bescherming persoonsgegevens. De bewerking, waaronder in ieder geval begrepen het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens, van dergelijke persoonsgegevens is aan regels gebonden met als oogmerk om de privacy van de betrokkenen te beschermen. Het gebruik van authentieke registraties, en gegevensuitwisseling in de publieke sector in het licht van dataprotectie (Wet bescherming persoonsgegevens) is uitgebreid onderwerp van studie geweest (zie onder meer Heemskerk, 2001).

In deze studie kiezen we echter niet het perspectief van privacy en dataprotectie, maar richten we ons op het gerelateerde begrip identiteit. We beschouwen het gebruik van gegevens over burgers vanuit het perspectief wat deze gegevens zeggen over het individu waarop de gegevens betrekking hebben. De gegevens representeren immers in mindere of meerdere mate het individu en dit heeft alles te maken met de identiteit van de betrokkene. Dat neemt overigens niet weg dat privacy en dataprotectie wel een rol spelen in de discussie.

2.2 Historische ontwikkeling[1]

Identiteit is een lastig concept, of misschien zelfs wel een familie van concepten. In de herfst van 2007 ontstond bijvoorbeeld beroering in de media naar aanleiding van uitspraken van prinses Maxima dat ze de Nederlandse identiteit nog niet had gevonden.[2] Culturele identiteit is slechts één van de dimensies van het begrip identiteit. Daarnaast bestaan ten minste persoonlijke, genetische, sociale en nationale identiteit. In deze studie zijn met name persoonlijke en sociale identiteit van belang.

Persoonlijke identiteit is een relatief nieuw begrip. In de pre-moderne tijd bestond het individu amper. Sociale klasse en rollen lagen grotendeels vast, er was weinig sociale mobiliteit en het individu bestond eigenlijk nauwelijks buiten een definitie waarin het individu fungeert als onderdeel van een systeem.

> *"The particulars of individual human experience were not important. The individual life was significant only as an example of the general struggle between good and evil, virtue and vice, faith and heresy, honour and disgrace" (Baumeister, 1986b).*

Individualiteit komt pas op in de Renaissance. Descartes, bijvoorbeeld, definieert individuen als denkende entiteiten met zelfbewustzijn. Zijn beroemde woorden 'ik denk dus besta ik' geeft uiting aan deze veranderde opvatting over het individu. Mensen zijn niet langer slechts marionetten, maar zelfbewuste individuen met een forse dosis zelfreflectie. In het latere Romanticisme wordt het idee van individualiteit verder versterkt doordat mensen zich meer bewust worden van hun uniciteit en daar ook toenemend uiting aan gaan geven. Kleding, bijvoorbeeld, is niet langer een uitdrukkingsvorm van lidmaatschap van een bepaalde klasse, maar veelmeer een expressie van de eigen voorkeuren. Persoonlijkheid in plaats van klasselidmaatschap wordt het dominante kenmerk van identiteit (Baumeister, 1986a). In de Victoriaanse tijd (grofweg van 1830-1900) groeit individualiteit verder uit. Urbanisatie verandert de positie van het individu in de maatschappij verder en individuele zelfontplooiing wordt een kernwaarde van het individu. Het verschil tussen publiek en privaat begint vorm te krijgen (huizen krijgen bijvoorbeeld meerder afsluitbare kamers, zie bijvoorbeeld Smith (2004)) en mensen trekken zich in toenemende mate terug in de privé sfeer.

In het begin van de 20e eeuw beginnen Amerikaanse pragmatisten te beseffen dat identiteit niet alleen in de hoofden van mensen zit (Descartes beeld over identiteit), maar dat onze identiteit ook wordt gevormd in interactie met onze omgeving. Identiteit is, met andere woorden, (ook) een sociaal construct. William James (1890), bijvoorbeeld, vraagt onze aandacht voor de verschillende posities en rollen die individuen in de maatschappij spelen:

---

1 Voor deze paragraaf is gebruik gemaakt van werk van Rachel Marbus, promotie onderzoeker binnen TILT.

2 Zie bijvoorbeeld <http://www.nrc.nl/binnenland/article1846825.ece/Maxima__Nederlandse_identiteit_nog_niet_ontdekt>.

> *"Many a youth who is demure enough before his parents and teachers, swears and swaggers like a pirate among his 'tough' young friends." (p. 295)*

In zijn perspectief hebben mensen verschillende identiteiten (social selves) afhankelijk van het aantal rollen en posities die ze spelen in het sociale leven. Hoewel James het begrip partiële identiteiten niet gebruikt zou hij er in retrospectief niet negatief tegenover staan. James onderkent dat de verschillende partiële identiteiten verschillende beelden van het individu kunnen oproepen en hij benadrukt dat doorgaans een van de deelidentiteiten dominant zal zijn: men is vooral onderzoeker, moeder of voetballer. Het beheren van onze deelidentiteiten culmineert, volgens James, in een 'truest, strongest and deepest self' van onze 'ideal social self'.

> *"This self is the true, the intimate, the ultimate, the permanent Me which I seek" (James, 1890, p. 317)*

Charles Cooley heeft het begrip *looking-Glass Self,* later hernoemd tot 'Empathic Introspection', geïntroduceerd waarmee hij aangeeft dat ons zelfbeeld wordt gevormd door vanuit het perspectief van een ander naar onszelf te kijken (Cooley, 1922). Identiteit wordt daarmee gevormd door sociale interacties met anderen.

George Herbert Mead plaatst identiteit in zekere zin terug in het brein. Mead beschrijft hoe identiteitsconstructie een interne dialoog is tussen "I" en "me" (Mead en Morris, 1934). Het "me" is het zelfbeeld dat onstaat als gevolg van het aannemen van het perspectief van de "generalised other", met andere woorden hoe relevante anderen over je denken. Het ik ("I") wordt gevormd door ingevingen van het individu. Het "I" vertegenwoordigt het individu als subject; met "me" als object. Het "I" is de 'kenner', het "me" is het 'gekende'. Deze noties liggen ten grondslag aan wat ICPP/SNG (2003) het "I" ('the indeterminate first person perspective'), het "Implicit Me" ('a person's own perception within a social setting'), en het "Explicit Me" ('the perception or representation of a person by others') noemen.

De rol van de ander in relatie tot identiteit is vooral uitgewerkt door de Canadese socioloog Erving Goffman in zijn invloedrijke boek 'The presentation of Self in everyday life' (Goffman, 1956). Goffman plaatst identiteitsconstructie in een toneelmetafoor. Hij stelt de relatie tussen het spelen van een rol (performance) en het toneel (front stage) centraal. Een sociale actor kan een toneel, attributen en uiterlijke kenmerken (kleding, make up, haardracht et cetera) kiezen om een bepaalde rol voor een bepaald publiek te spelen. Een organisatie adviseur die op zijn eigen kantoor in een spijkerbroek rondloopt, kan er bijvoorbeeld voor kiezen om naar een klant een pak aan te doen, haren te kammen en baard te scheren.

Tijdens het spelen van een bepaalde rol zal een individu proberen coherent en consistent over te komen en zich aan de situatie aan te passen. Tijdens de 'voorstelling' presenteren individuen zichzelf bewust ('information given'), maar geven ze ook onbewuste signalen af ('information given off'). Het feit dat een

stropdas niet goed gestrikt is of er een ladder in een kous zit kan onopgemerkt zijn door de 'acteur', terwijl het publiek het wel ziet en er het zijne van denkt (wat een sloddervos).

Identiteit in Goffman's perspectief bestaat uit de rollen die mensen spelen (hun voorstellingen) en het beeld dat zij van zichzelf presenteren (hun "front"). Het front bestaat uit de context, objecten, meubilair, achtergrond, maar ook uit persoonlijke attributen, zoals kleding, sociale positie, leeftijd, geslacht, lichaamstaal etc. Alles bij elkaar draagt bij aan het beeld dat een toeschouwer heeft over het individu.

Een ander centraal thema in Goffman's analyse is publiekscheiding ('audience segregation'). Mensen spelen verschillende rollen en hebben derhalve verschillende partiële identiteiten (vgl. James). Identiteit bestaat volgen Goffman uit de som van alle deelidentiteiten van een individu. Individuen worden in hun gedrag in een bepaalde rol geleid door de context; de situatie, wie aanwezig is en wie niet, en de daarin geldende normen en verwachtingen bepalen hoe mensen zich gedragen. Het van elkaar kunnen scheiden van de verschillende publieken en contexten is van wezenlijk belang om verschillende rollen te kunnen spelen in het maatschappelijk verkeer. Het feit dat een vooraanstaand politicus gepassioneerd miniatuurspoor hobbyist is, en zich tijdens zijn hobby zelfs in klassiek conducteurspak inclusief rode pet hijst, draagt niet bij aan zijn gezag in de ministerraad en hij doet er dus goed aan deze informatie niet te delen met anderen dan zijn railhobby vrienden.

Een belangrijke rode draad in het werk van de pragmatisten is dat zij het idee delen dat identiteit bestaat uit een verzameling deelidentiteiten die zich ontwikkelen in specifieke contexten en dat deze deelidentiteiten gescheiden moeten blijven.

In het begin van de jaren 80 verandert het beeld over identiteit als gevolg van maatschappelijke en technische ontwikkelingen wederom. De opkomst van de informatiemaatschappij (Castells, 1996, 1997, 1998) speelt hierbij een centrale rol. Laat moderne en post moderne filosofen, zoals Anthony Giddens, nemen het idee van het bestaan van verschillende deelidentiteiten en de fragmentatie van deze deelidentiteiten over, maar erkennen ook dat het individu niet geheel vrij is in de constructie van haar identiteit, ook niet in sociale interactie. Identiteit kent continuïteit.

> *"A person's identity is not to be found in behaviour, nor - important though this is - in the reactions of others, but in the capacity to keep a particular narrative going. The individual's biography, if she is to maintain regular interaction with others in the day-to-day world, cannot be wholly fictive. It must continually integrate events which occur in the external world, and sort them into the ongoing 'story' about the self." (Giddens, 1991)*

Dit narratieve aspect van identiteit zien we ook duidelijk terug in het werk van Paul Ricoeur. Persoonlijke identiteit in zijn perspectief wordt ontwikkeld in een narratieve symbolische representatie. Taal en verhaal spelen hier dus een centrale

rol. We ontdekken, of vinden, onze identiteit door naar ons eigen verleden te kijken.

> *"The narrative constructs the identity of the character, what can be called his or her narrative identity, in constructing that of the story told. It is the identity of the story that makes the identity of the character" (Ricoeur, 1990 (1992), pp 147-148)*

Latere filosofen zoals Kenneth Gergen en W.T. Anderson onderkennen dat het erg lastig voor individuen is om coherentie te bewaren in hun deelidentiteiten. Zij verlaten het idee van 'unified egos' – enkelvoudige coherente zelfbeelden (Gergen, 2009). Gergen (Gergen, 1991) beschrijft wat hij noemt de 'sociale saturatie' die resulteert van de technologisch gemedieerde interactie met steeds meer anderen. Mensen verkeren in een constant proces van constructie en reconstructie van hun identiteit en kunnen weliswaar naar de buitenwereld coherent overkomen, maar voor zichzelf zijn ze meer en meer multifrenisch (Gergen, 1991). Hij ziet deze multifrenie als problematisch omdat hij veronderstelt dat veel mensen problemen hebben met het heen en weer schakelen tussen de verschillende deelidentiteiten in kort tijdsbestek. Het idee van deelidentiteiten is volgens hem overigens niet problematisch, zolang we maar voldoende tijd hebben om van toneel te wisselen.

Wat de laat moderne filosofen ons leren is dat het idee van een enkelvoudige, coherente identiteit plaats gemaakt heeft voor minder coherente en meervoudige identiteiten die door het individu worden aangenomen afhankelijk van de situatie. Het schakelen tussen de verschillende deelidentiteiten wordt steeds dynamischer door nieuwe technologieën ("nu even niet schat, ik ben aan het vergaderen"). Tijd en plaats demarqueren niet langer de verschillende contexten en rollen waarin we opereren. Vooral mobiele telefoons brengen vroeger door ruimte gescheiden contexten bij elkaar (denk aan telefoongesprekken in de trein, maar we dergelijke contextschakelingen veelvuldig kunnen aanschouwen).

Sherry Turkle (1997) laat zien hoe ons gebruik van computers resulteert in een 'decentered self' omdat verschillende parallelle identiteiten in verschillende contexten tegelijkertijd actief zijn. We hebben een online identiteit ('life on the screen') die gezien kan worden als 'multiple distributed system' en die samenvloeit met onze off-line identiteit. Zoals een van Turkle's respondenten het zegt (Turkle, 1997):

> *"I split my mind. I'm getting better at it. I can see myself as being two or three or more. And I just turn on one part of my mind and then another when I go from window to window. I'm in some kind of argument in one window and trying to come on to a girl in a MUD in another, and another window might be running a spreadsheet program or some other technical thing for school.... And then I'll get a real-time message [...] and I guess that's RL (Real Life). It's just another window. Real life is just one more window, he repeats, and it's not usually my best one" (p. 13).*

Tot nu toe is het betoog over opvattingen over wat identiteit is geplaatst in het licht van het tonen van verschillende gezichten, rollen en uitdrukkingen van individuen en hoe deze interacteren met de omgeving en hoe dit in de loop der tijd is veranderd. Er is echter ook een ander aspect van identiteit dat moet worden betracht. Identiteit verwijst ook naar 'hetzelfde' zijn. De term identiteit komt van het Latijnse 'identitas' wat afstamt van het latijnse woord 'idem' dat 'zelfde' betekent. Identiteit verwijst in dit opzicht naar hetzelfde individu dan voorheen (eerste persoons perspectief, of ik-perspectief). Gelijkheid speelt ook een rol in het perspectief van de derde. We zijn in staat om een bekende te herkennen omdat deze hetzelfde is als voorheen, hun identiteit is constant (persistent), zij het dat deze door de tijd wel gradueel verandert. We zijn ook in staat om een persoon die we 'kennen' aan te wijzen in een massa door deze persistentie van identiteit. Anders gezegd, we kunnen individuen die we kennen identificeren aan hun identiteit. Iemands identiteit kennen betekent daarmee dat we voldoende informatie over dit individu hebben om de connectie te leggen tussen een beeld en een individu in Real Life die past bij dit beeld.

Paul Ricoeur heeft zich uitgebreid met deze verschillende identiteitsconcepties bezig gehouden. Hij onderscheidt 'ipse identiteit' en 'idem identiteit'. Ipse identiteit (oftewel 'selfhood') verwijst naar het zelfbeeld ('sense of self' – 'ipse') van een individu dat reflecteert wie deze persoon werkelijk is en dat wordt gevormd door een dynamische continue zelfrepresentatie (het narratief). Idem identiteit verwijst naar gelijkheid (idem). Dit kan zich uiten in een numerieke gelijkheid (uniciteit), een kwalitatieve gelijkheid (gelijkenis) en een ononderbroken continuïteit of een ontbreken van variatie of ontbreken van verscheidenheid. Gelijkheid kan bijvoorbeeld bestaan uit een unieke digitale identiteit die statisch is, maar ook periodiek geactualiseerd kan worden. De notie van idem identiteit is verwant aan identificatie (extern perspectief), terwijl ipse identiteit behoort tot de innerlijke wereld van het individu. Dat betekent niet dat idem een externe identiteit is en ipse een interne identiteit omdat we om een 'self' te ontwikkelen we het externe perspectief moeten internaliseren (Hildebrandt, Koops en de Vries, 2008).

> *'Idem-identity is the third-person attribution of sameness: 'This is Miss Cheung, a blond female executive'; it takes an objectified perspective. Ipse-identity depends on a first-person perspective on what constitutes oneself as a continuous being in the course of time, while experiencing multiplicity and difference in the here and now: 'I am Li-lian, a feminist and executive, even if this male bully is treating me right now as a secretary'; this takes a subjective perspective. These two processes cannot be reduced to each other and actually depend on each other.' (Hildebrandt, Koops, 2008)*

2.3 Conclusie

Dit korte overzicht van het denken over identiteit door de (filosofische) geschiedenis heen laat zien dat identiteit een complex concept is. Hoewel we gewend zijn te spreken van iemands identiteit alsof dat een enkelvoudig concept is, is het zinvol onderscheid te maken in deelidentiteiten die elk in verschillende contexten worden getoond. Iedere deelidentiteit wordt in een bepaalde context ontwikkeld in interactie met de omgeving volgens de regels en verwachtingen binnen die context. Deelidentiteiten hebben een zekere stabiliteit, maar veranderen ook in de loop der tijd. Omdat deelidentiteiten verbonden zijn aan een context is het beeld dat wordt geprojecteerd onderhevig aan interpretatie. Interpretatie van context en projectie maakt dat het beeld klopt (collega Sjaak in boerenkiel betekent niet dat hij boer is geworden, of gek, maar gegeven de tijd van het jaar (Februari) en de locatie (Tilburg) slechts dat hij (waarschijnlijk) carnaval viert).

De moderne mens schakelt betrekkelijk eenvoudig tussen de verschillende deelidentiteiten (multifrenie). ICT speelt in dit schakelproces tussen de verschillende deelidentiteiten een centrale rol omdat het ruimte en tijd eenvoudig kan overbruggen. Als gevolg hiervan zijn sociale contexten snel en eenvoudig te wijzigen, met alle sociale gevolgen van dien voor degenen die geen deel uitmaken van de contextwisseling (denk aan telefoongesprekken in de trein die voor de niet deelgenoten in dezelfde coupé vaak onplezierig zijn).

3. Digitale identiteiten

3.1 Inleiding

Ook in de online wereld kunnen we in meerdere betekenissen spreken van identiteiten. In virtuele werelden, zoals Second Life, ontwikkelen de 'spelers' een aparte identiteit. De speler construeert letterlijk haar 'tweede' identiteit door een Avatar op te bouwen. De Avatar krijgt een uiterlijk met fysieke dimensies en kenmerken, geslacht, lengte, bouw, haarkleur, kleur ogen en dergelijke. Ook wordt de Avatar een garderobe aangemeten. Het proces van identiteitsconstructie zoals dat we dat in het vorige hoofdstuk hebben gezien vindt daarmee ook in dergelijke virtuele werelden plaats. Het individu beoogt een bepaald beeld van haarzelf te presenteren en zal zich daartoe een bepaald uiterlijk aanmeten, bepaalde kleding en attributen dragen en zich op een bepaalde manier gedragen. Ze zal haar gedrag en uiterlijk ook aanpassen op basis van de reacties van anderen in de virtuele wereld. Hoewel veel bewoners van virtuele werelden zichzelf nabouwen in de virtuele omgeving zijn er ook die nadrukkelijk kiezen voor een totaal andere identiteit. Avatar en 'poppenspeler' zijn soms onherkenbaar verschillend (zie bijv. Cooper, 2007).[3]

Op online Social Network Sites (profielsites) zoals Hyves, Myspace, Facebook en dergelijke onderhouden de gebruikers eveneens identiteiten. Met zorg en aandacht, al zou je dat soms gezien de lay-out van de profielen niet altijd zeggen, wordt een online identiteit ontwikkeld en onderhouden (boyd, 2007, Donath en boyd, 2004, Turkle, 1997). Maar ook in andere online en digitale domeinen kan worden gesproken van digitale identiteiten. In de afgelopen decennia is een ontwikkeling te onderkennen van eenvoudige gegevensverzamelingen over individuen in de richting van gegevensverzamelingen die een rijke representatie vormen van de betrokkenen en die we daarom gedigitaliseerde identiteiten kunnen noemen. Deze digitale identiteiten fungeren doorgaans als passieve representaties van individuen, maar het valt te verwachten dat ze ook actief namens hun spiegelbeeld in de fysieke wereld handelingen zullen gaan verrichten. In dit hoofdstuk beschrijven we de ontwikkeling van records, via digitale identiteiten naar actieve digitale agents.

3 Denk aan de zogenaamde 'Furries' in Second Life.

3.2 Van record naar digitale identiteit

Iedere organisatie die mensen als klant of cliënt heeft zal gegevens over die personen bijhouden. In het informatietijdperk bestaan die gegevensverzamelingen uit geautomatiseerde databestanden. In de meest eenvoudige vorm bestaat een databestand uit een verzameling records die elk een aantal (doorgaans gelijke) attributen (velden) bevat die van belang zijn voor een primair proces van de de beheerder van het databestand. Welke attributen worden bijgehouden is afhankelijk van dat primaire proces. Het aantal en de aard van de bijgehouden attributen hoort op basis van de Wet bescherming persoonsgegevens relevant en minimaal te zijn in het licht van het doel waarvoor de gegevens worden verzameld.[4] Het ledenbestand van een dartvereniging zal daarom bijvoorbeeld alleen de attributen naam, adres en telefoonnummer en betaalstatus behoren te bevatten omdat deze voldoende zijn om het clubblaadje rond te sturen, bij te houden wie het blaadje eigenlijk niet meer zou moeten krijgen en de wekelijkse dartavond te annuleren.

De records in zo'n databestand bevatten informatie over een bepaalde groep personen en de individuen binnen die groep. Omdat het in veel gevallen gaat om een zeer beperkte hoeveelheid gegevens die wordt bijgehouden spreken we in deze gevallen van arme digitale identiteiten. De gebruiker van de gegevens kan zich op basis van de gegevens namelijk nauwelijks een beeld vormen van de geregistreerde personen. Identiteit zoals in het voorgaande hoofdstuk beschreven betreft een rijker beeld van het individu dan alleen naam en contactgegevens. Naarmate er meer gegevens deel uitmaken van het record over een individu in een gegevensbestand wordt de identiteit rijker. Digitale identiteit is daarmee een gradueel concept.

In formele zin definiëren Pfitzman en Hansen (2008) identiteit dan ook als:

> *"[A]n identity is any subset of attributes of an individual which uniquely characterises this individual within any set of individuals."*

Ook Hildebrandt en Koops (2008) hanteren een identiteitsdefinitie die uitgaat van een gegevensverzameling:

> *"[T]he term identity is often used to refer to the unique set of attributes that makes up a particular person, to which an identifier refers by using a subset of attributes that is sufficiently discriminating to individuate a subject. In that case the identity of the person is understood as the complete set of attributes which uniquely describes her and this is what the identifier (often also called identity) refers to."*

4 Indachtig de artikelen 6, 7 en 8 van de Wbp.

Ook in de online wereld bestaat een groot aantal databestanden over klanten, gebruikers, cliënten, etc. Klanten van een online winkel hebben doorgaans een 'account' bij die winkel. Dit account is toegankelijk door middel van, bijvoorbeeld, een user name en password. Deze kunnen door de gebruiker worden gebruikt om zichzelf te authenticeren voor de betreffende dienstverlener waarmee deze toegang krijgt tot diens gegevens zoals bijgehouden door de dienstverlener. Die gegevens liggen vast in records, net zoals hierboven is beschreven voor gegevensbestanden in gebruik bij organisaties in de fysieke wereld.

Het is belangrijk om op dit punt te wijzen op verschillende noties van identiteitsmanagement die hier bij elkaar komen: een ICT beheer perspectief en een meer sociologisch getint perspectief dat aansluit bij het vorige hoofdstuk. In het ICT beheer perspectief worden de records waarover we hiervoor hebben gesproken aangeduid als identiteiten. De gebruiker creëert een elektronische identiteit (account) bij de dienstverlener (service provider) en de toegang (authenticatie, identificatie, verificatie, autorisatie, of in het algemeen 'access control') en het beheer van die identiteit wordt dan ook identiteitsmanagement genoemd. In deze technische benadering van identiteitsmanagement gaat het om het beheren van de rechten van gebruikers tot bepaalde voorzieningen en gaat het niet om aspecten van identiteitsmanagement zoals impressiemanagement zoals dat in het vorige hoofdstuk is beschreven. Dat laatste past binnen het meer sociologische perspectief op identiteitsmanagement. Hieronder zullen we zien dat naarmate een digitale identiteit rijker wordt in termen van informatie die het bevat over een concrete persoon, deze meer en meer het sociologische perspectief binnen schuift.

Gegevensverzamelingen kunnen uiteraard veel rijker zijn, of een veel rijker beeld geven van de geregistreerde individuen dan in het dartclub voorbeeld is beschreven. Amazon houdt bijvoorbeeld veel meer informatie bij over haar klanten en hun gedrag. Amazon beschikt over allerhande contactgegevens, betaalkaartgegevens, leeftijd, geslacht en dergelijke. Maar belangrijker is nog dat Amazon de aankoophistorie van haar klanten bijhoudt alsmede wat klanten op de website doen. Het zoekgedrag en doorklikgedrag wordt bijgehouden omdat dit iets vertelt over de interesse van gebruikers en die informatie kan worden gebruikt om aankooptips te geven. Amazon verkrijgt door het gedetailleerd volgen van hun gebruikers een veel rijker beeld van haar klanten dan de dartclub van haar leden heeft (op basis van het ledenbestand). Amazon weet bijvoorbeeld dat Ronald en Simone iets hebben met privacy en identiteitsmanagement aangezien ze een aantal boeken over die thema's hebben aangeschaft. Ook is het Amazon niet ontgaan dat Ronald een redelijk omvangrijke collectie Philip K. Dick SciFi boeken heeft (en DVDs met op deze boeken gebaseerde films) en dat Simone blijkbaar fervent lezer van Engelse en Amerikaanse detectives is. Amazon heeft daarmee een beeld van onze interesses en bovendien van een deel van onze identiteit. Naarmate we meer bij Amazon winkelen (zowel rondkijken als kopen) krijgt Amazon een rijker beeld van ons. Onze identiteit zoals gezien door Amazon wordt rijker waardoor Amazon beter in staat is om aanbiedingen te doen die bij ons passen[5].

5 Zie bijvoorbeeld wat Amazon.com hierover meldt op <http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496>.

De ontwikkeling van eenvoudige records naar rijke identiteiten kan ook worden waargenomen in de publieke sector. De hoeveelheid persoonlijke data in de GBA is – hoewel zeer relevant – redelijk beperkt. Tal van afnemers gebruiken de data in hun bedrijfsprocessen en verrijken deze met andere noodzakelijke data om publieke diensten te kunnen verstrekken aan burgers. Zo zal de Informatie Beheer Groep bij studenten gegevens opvragen over hun woon– en financiële situatie, studie, onderwijsinstelling, etc. De UWV heeft behoefte aan informatie over werk– en woonsituatie, ziekte, financiële situatie, etc. Een groeiende complexiteit van het maatschappelijke en beleidslandschap betekent een toename in de door de overheid geregistreerde hoeveelheid gegevens over burgers. Deze gegevens worden in gedigitaliseerde informatieprocessen verwerkt en gekoppeld aan elektronische authenticatiemechanismen zoalsPKIOverheid en DigiD. Bovendien zien we in de publieke sector vergelijkbare ontwikkelingen als in de private sector zoals bij Amazon. De publieke dienstverlening wordt op bepaalde punten gepersonaliseerd, dat wil zeggen toegesneden op de behoeftes en interesses van de burger. Vaak geeft de burger zelf aan wat hem wel of niet interesseert (bijvoorbeeld publieke informatie over zijn wijk of regio), maar het is ook mogelijk dat de overheid meer proactief data verzamelt en koppelt. Aldus worden de identiteiten van burgers steeds rijker. Roger Clarke (1994) spreekt in dit verband van een *digital persona*:

> *"[A] model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual."*

In deze definitie zijn verschillende elementen van belang. In de eerste plaats gaat het om de '*public personality*' van individuen. Met andere woorden het gaat om kenbare kenmerken van het individu. Deze kunnen eenvoudig en objectief waarneembaar zijn: kleur ogen, aankoop van een bepaald product, maar kunnen ook interpretatie vergen, bijvoorbeeld wanneer iets wordt vastgelegd over het soort mens (SciFi geïnteresseerde of detectivelezer) dat iemand is of zou kunnen zijn. Een tweede element is dat het gaat om data (ook wel attributen genoemd), met andere woorden om zaken die zijn vast te leggen in een IT systeem. In termen van Riceour's onderscheid in *idem* en *ipse* identiteit heeft de digital persona dus betrekking op *idem* identiteit. De data die onderdeel uitmaakt van het digital persona is ontstaan doordat er een noodzaak was binnen een bepaald proces om deze te verzamelen en vast te leggen, zoals in de eerdergenoemde voorbeelden van de IB groep en UWV. De data wordt verzameld met als doel te worden gebruikt als *representatie* van het individu, bijvoorbeeld als student of uitkeringsgerechtigde. Het gaat er dus uitdrukkelijk om te dienen als representatief beeld van een persoon (voor een bepaald doel of in een bepaalde context) om op basis daarvan te handelen of beslissingen te nemen over dit individu. Clarke's 'digital personae' zijn door het feit dat ze fungeren als representaties van individuen in de fysieke wereld 'volwaardige' identiteiten.

Clarke (1994) maakt onderscheid tussen '*projected*' en '*imposed personae*'. Het '*projected persona*', is het beeld dat door het individu bewust of onbewust wordt geschapen naar de buitenwereld. De data die het individu aanlevert in een

bepaalde transactie, bijvoorbeeld de voorkeuren die een klant van Amazon opgeeft in haar klantenprofiel, maken deel uit van dit geprojecteerde beeld. Het individu heeft tot op zekere hoogte controle over wat wordt bijgedragen aan zijn of haar 'projected digital persona'. Ook Avatars, en profielpagina's op Hyves zijn voorbeelden van 'projected personae'.

Van een 'imposed persona' is sprake wanneer het persona bestaat uit data die ontstaat door interpretatie van de houder van het persona over het betreffende individu. De data die Amazon verzamelt op basis van het surfgedrag van haar klanten, en vooral de consequenties voor het individu die Amazon hieraan verbindt – bijvoorbeeld het tonen van een op de interesses van de persoon toegespitst aanbod – zijn onderdeel van 'imposed personae' van deze klanten. Amazon creëert dus een beeld van haar klanten, in plaats van dat dit beeld primair door de klanten wordt gecreëerd. In feite gaat het in dit geval om een hybride persona aangezien de klant bepaalde gegevens aanlevert en Amazon daar gegevens en beoordelingen aan toe voegt. Er zijn ook 'zuivere' 'imposed personae'. 'Credit rating agencies' zoals Experian[6], verzamelen informatie over burgers zonder dat deze daar zelf bij zijn betrokken.

Aangezien vele organisaties 'digitale personae' opbouwen en onderhouden spreekt Clarke van 'imposed digital personae', terwijl hij geneigd is te spreken van een enkele 'projected digital persona' (1994). In onze optiek is dat niet geheel juist en zijn wij geneigd zijn te stellen dat een individu ook verschillende 'projected personae' heeft, afhankelijk van context en doel. Ronald's Second Life Avatar is een 'projected persona' (die toevallig veel rood haar heeft, terwijl Ronald in de fysieke wereld eerder kampt met kalend peper en zout kleurig haar). Simone toont op Hyves heel andere (meer persoonlijke) kanten van zichzelf dan op het professionele online netwerk LinkedIn. Dit raakt aan Goffman's idee van 'audience segregation': we spelen verschillende rollen afhankelijk van het te verwachten publiek. In dit geval spreken we dan ook van 'deelidentiteit' of 'digitale deelidentiteit', indien het 'spel' zich online afspeelt. We spelen verschillende rollen afhankelijk van de context en setting waarin we ons bevinden. Dit geldt niet alleen in de offline wereld maar ook online. De idee van 'deelidentiteiten' is door Giddens en Turkle doorgetrokken naar de informatiesamenleving waarbij zij de nadruk leggen op een groeiende fragmentatie van de persoonlijke identiteit en het parallel lopen van verschillende deelidentiteiten in de online (en offline) wereld. Het construct identiteit wordt minder coherent als gevolg van nieuwe communicatietechnologieën en de uiteenlopende online levens die we leiden en op zekere momenten interfereren met onze rollen in het offline bestaan.

6 Zie bijvoorbeeld <http://www.experian.nl/>.

3.3 Digitale identiteit komt tot leven

Ofschoon gegevens over burgers altijd van belang zijn geweest voor de overheid en derhalve werden geregistreerd, worden eenvoudige records nu omgevormd tot steeds complexere identiteiten die een meer en meer compleet (ook: holistisch) beeld van burgers geven. Tot voor kort werden rijkere identiteiten samengesteld uit data op verzoek van de overheid afkomstig van burgers zelf of de door de betreffende publieke instantie gegeven interpretaties daarvan. Nieuwe technologieën, denk aan smart cards, RFID, GPS, biometrie, maken het mogelijk dat ook andere databronnen worden gevonden en gecombineerd. Dit betekent dat nieuwe soorten van data worden gegenereerd en gebruikt door de overheid. Daarnaast publiceren burgers zelf steeds meer gegevens online, de eerdergenoemde 'projected digital personae', die mede beschikbaar zijn voor de overheid. Het is geen geheim dat de Belastingdienst met het oog op het opsporen van fraude informatie over burgers zoekt op Hyves[7].

Na een periode waarin de overheid minder over haar burgers wist doordat digitale data opslag duurder was dan opslag van gegevens op papier,[8] hebben de ICT en netwerk revoluties het mogelijk gemaakt om grote hoeveelheden gegevens over burgers en klanten te verzamelen. Dit aanbod heeft in zekere zin een vraag naar een grotere data-intensiteit (meer data, nieuwe data) binnen de overheid in de hand gewerkt. De behoefte bij de overheid aan meer data is ook om andere redenen gegroeid, hoewel lastig is vast te stellen of dit ook het geval zou zijn geweest zonder ICT revolutie. Er is bijvoorbeeld een groeiende aandacht voor veiligheid en handhaving en meer algemeen de drang in onze moderne samenleving om (potentiële) risico's zo nauwkeurig mogelijk in te schatten en liefst te ondervangen (Garland, 2001, Giddens, 1999). Of het nou gaat om criminaliteitsbestrijding of jeugdbeleid, steeds vaker ligt de nadruk op het voorkomen van schadelijk, deviant of illegaal gedrag in plaats van op repressie of remedies achteraf. Deze tendens is alomtegenwoordig en bestrijkt derhalve een groot aantal beleidsterreinen van de overheid. Het risicodenken past bovendien binnen de rijzende overtuiging dat we de samenleving kunnen programmeren zodanig dat sociale problemen verdwijnen. Ofwel het denkbeeld dat onze samenleving maakbaar is heeft (wederom) postgevat in overheidsbeleid. Als gevolg van deze ontwikkelingen evolueert het eenvoudige record dat relevante kenmerken van een burger in een bepaalde, beperkte context bevat in representatie van die persoon bestaande uit een veelheid aan individuele kenmerken, rapportages over gedragingen en conclusies over feiten en observaties. Niet alleen wordt de hoeveelheid data die wordt vastgelegd steeds groter, maar ook ontstaat er een kwalitatieve verschuiving. Het gedetailleerde beeld dat van de burger wordt opgebouwd in moderne databanken bestaat niet alleen uit feiten, maar meer en meer ook uit al dan niet automatisch getrokken conclusies over gedrag en mogelijk toekomstig gedrag. Hiertoe wordt gebruik gemaakt van complexe en geavanceerde

7 Aldus <http://www.volkskrant.nl/binnenland/article508021.ece/Belastingdienst_struint_rond_op_Hyves>.

8 De oude, handgeschreven, bevolkingsregisters bevatten veel informatie in de marges die werd gebruikt in aanvulling op de officiële gegevens.

data-analyses. Hierdoor kan nieuwe kennis over individuele burgers en groepen burgers worden gegeneerd, op basis waarvan bijvoorbeeld uitspraken kunnen worden gedaan over het type persoon dat de burger is, of zou kunnen zijn, en de (potentiële) risico's die daaraan verbonden zijn (risico profilering). Aan bepaalde kwalificaties worden vervolgens weer conclusies verbonden, bijvoorbeeld dat nauwere observatie moet plaatsvinden wanneer bepaalde financiële transacties hebben plaatsgevonden.[9] Door slimme berekeningen kunnen dan niet alleen voorspellingen worden gedaan over de interesses van Ronald of Simone in een zeker genre boeken of bepaalde vormen van publieke informatie, maar ook over de mate van (on)waarschijnlijkheid dat zij fraude zullen plegen met gemeenschapsmiddelen of een snelheidsovertreding begaan.

Ofschoon profilering bij de Nederlandse overheid nog nauwelijks of slechts in beperkte mate plaatsvindt, tekent zich een begin af met vergaande invoering van deze werkwijzen in het justitieel en politieel domein. De Raad van Hoofdcommissarissen zet bijvoorbeeld in op de mogelijkheden van 'nodal' en 'intelligence led policing' om de effectiviteit van de politie te vergroten (Projectgroep Visie op de politiefunctie, 2005). Het is belangrijk te beseffen dat het niet alleen gaat om informatie over het individu zelf waarover conclusies worden getrokken die effecten hebben voor dit individu, maar dat ook informatie over anderen daarbij wordt gebruikt. Al dan niet vermeend groepslidmaatschap wordt gebruikt om conclusies die kunnen worden getrokken over een bepaalde groep te projecteren op het individu (groepsprofilering). Het feit dat een bepaalde burger in een postcodegebied woont met een laag gemiddeld inkomen wordt in de private sector bijvoorbeeld gebruikt om inwoners van zo'n postcodegebied voorzieningen (bijvoorbeeld Wehkamp aankopen) te onthouden, ook al kan een individuele inwoner van zo'n gebied best kapitaalkrachtig zijn.

De idee dat meer informatie meer effectiviteit oplevert in het realiseren van beleidsdoeleinden in uiteenlopende contexten, betekent bovendien dat eenmaal aangelegde verzamelingen van data steeds meer gebruikers trekken. Digitalisering houdt mede in dat pakketten informatie over individuen (die we dus kunnen bestempelen als identiteiten) steeds eenvoudiger kunnen worden gedeeld en samengevoegd met informatie over diezelfde individuen bij andere instanties. Met andere woorden, eenvoudige records of deelidentiteiten worden samengesmeed tot context-overschrijdende, integrale representaties van de burger. Een goed voorbeeld is het Elektronisch Kind Dossier dat in aanleg is gericht op digitalisering van de jeugdgezondheidszorg maar inmiddels een sterk aanzuigende werking vertoont ten aanzien van andere organisaties (maatschappelijk werk, scholen, politie, rechterlijke macht) die zich op enige wijze bezig houden met het welzijn van jongeren.

9 Een voorbeeld uit de private sector is het volgende voorval. Op een zeker moment heeft een van de auteurs van dit rapport meerdere vliegtickets achter elkaar geboekt voor congressen en buitenlandse vergaderingen in de twee manden na de boeking. Nog geen vijf minuten na het boeken van de derde vlucht werd de auteur gebeld door zijn/haar creditcard maatschappij met de vraag of hij/zij haar kaart kwijt was omdat er verdachte boekingen plaatsvonden. Kennelijk monitort de creditmaatschappij transacties in real-time om bepaalde vormen van fraude te kunnen detecteren.

3.4 Een eigen leven

De steeds rijker wordende digitale identiteiten gaan een eigen leven leiden. Niet langer is het nodig dat de burger zich tot de overheid vervoegt om een bepaalde voorziening te verkrijgen (aanvraag van een subsidie, uitkering of vergunning). Naarmate het beeld van de burger bij de overheid 'completer' wordt, kan de overheid meer en meer handelen op basis van deze digitale representatie. De benodigde informatie voor het nemen van bepaalde beslissingen wordt met andere woorden niet meer aangeleverd door de burger zelf, maar wordt onttrokken van haar digitale evenknie. De digitale identiteit gaat fungeren als vertegenwoordiger of 'proxy' (Clarke (1994)) die als passieve entiteit wordt uitgelezen. Pro-actieve dienstverlening is hiervan een tastbaar voorbeeld. Informatie over de leefsituatie van een burger als onderdeel van haar digitale identiteit kan worden gebruikt om pro-actief de kinderbijslag te verhogen wanneer zij middels haar dataset (attribuut kinderen wordt aangepast) kennis geeft van het blijde nieuws van een tweede of derde nakomeling. Het nieuws over nieuwe dochter of zoon wordt niet door de moeder van vlees en bloed verstrekt aan de SocialeVerzekeringsbank, maar wordt in de gemeente waar zij aangifte van de geboorte doet onderdeel van haar digitale identiteit waarna 'deze' vervolgens een signaal afgeeft aan de SVB die weet wat haar te doen staat. In dit geval vindt de handeling van informatieverstrekking aan de SVB metaforisch plaats via de bij de woongemeente geregistreerde bevolkingsgegevens, maar wanneer we de verschillende databestanden niet langer beschouwen als afzonderlijke bestanden, maar gezamenlijk als digitale identiteit dan is het hierboven beschreven proces niet langer vreemd.

Met andere woorden, identiteiten worden voortdurend rijker en komen tegelijkertijd meer en meer los te staan van de persoon van vlees en bloed die erdoor wordt gerepresenteerd. Nu meer dan vroeger, aangezien het contact tussen overheid en burger wordt gedigitaliseerd en vaker op afstand plaatsvindt. De burger transformeert zo in een digitale dataset waarop de overheid haar beslissingen baseert. Besluitvormingsprocedures worden bovendien steeds vaker geautomatiseerd, waardoor menselijke betrokkenheid geheel wegvalt.

In eerder onderzoek hebben we dit geabstraheerde identiteiten genoemd (van der Hof, Leenes en Fennell, 2009). Digitale identiteiten worden opgebouwd uit attributen die naar ons verwijzen, maar vervolgens wordt de relatie met de persoon losgelaten. De overheid weet steeds meer over ons, maar kent ons natuurlijk niet echt. Ondanks de groeiende data-intensiteit lijkt de afstand tussen overheid en burger alleen maar groter te worden. De geabstraheerde digitale identiteiten, bijvoorbeeld persoonlijke profielen of risicoprofielen, gaan een eigen leven leiden, want ze worden gebruikt los van de persoon voor wie ze model staan. We keren weer even terug naar Clarke (1994) en zijn 'digital persona', waarover hij verder zegt:

> *"There is something innately threatening about a persona, constructed from data, and used as a proxy for the real person. It is reminiscent of the popular image of*

the voodoo doll, a (mythical) physical or iconic model, used to place a magical curse on a person from a distance. [...] Some people may feel that it is demeaning, because it involves an image rather than a reality. Others may regard it as socially dangerous. This is because the person's action is remote from the action's outcome. This frees the individual's behaviour from his or her conscience, and hence undermines the social constraints which keep the peace."

Los van de afstand die wordt gecreëerd, kunnen geabstraheerde digitale identiteiten mettertijd bovendien hun representativiteit verliezen en tot verkeerde (overheids)beslissingen leiden. Van der Hof en Keymolen (2010) spreken van identiteit die versteent in het systeem, terwijl real-life identiteiten zich met een zekere dynamiek blijven door ontwikkelen. Het gevolg is dat de persoon waaraan wordt gerefereerd niet langer adequaat wordt vertegenwoordigd door de dataset.

Omgekeerd komt ook voor; vanuit het systeem wordt dynamiek van het individu verondersteld en de procedures zijn dan ook soms gericht op actualisering van de digitale identiteit, zelfs wanneer sommige zaken niet veranderen in de werkelijkheid. Het rapport Kafka in de Polder geeft daarvan een wrang voorbeeld (de Jong et al., 2008).

"Een gehandicapte man is jaren geleden beide benen, tot ver boven de knieën, kwijtgeraakt. Hij vertelt dat hij toch nog regelmatig opnieuw moet bewijzen dat hij gehandicapt is. Baliemedewerkers verontschuldigen zich soms voor de regels, maar eisen elke keer een recent bewijs van invaliditeit. Ook als de man al jaren bekend is aan dat loket. Een nieuwe aanvraag is een nieuwe aanvraag en kennelijk moet dan alles weer opnieuw bekeken worden. Voor de man in kwestie is dat raar: 'Ze denken bij de gemeente zeker dat ze weer aangroeien'." (de Jong et al., 2008 p. 13.)

Deze fenomenen raken in bredere zin aan kwesties als datakwaliteit en systeemtransparantie. Om beslissingen te kunnen nemen moet de overheid erop kunnen vertrouwen dat de gegevens aan de bron correct zijn. Het systeem van basisregistraties bevat mechanismen (terugmeld– en correctieplichten) die dit moeten waarborgen, maar zoals altijd is de praktijk weerbarstig. Wanneer besluiten worden genomen in ketens van publieke instanties blijken deze mechanismen niet altijd goed te werken. Als een afnemer van data fouten in data moet terugmelden, waar ligt dan de verantwoordelijkheid als er niet één, maar een reeks afnemers is (Hof et al., 2008). Een recent rapport van de Nationale Ombudsman (2009) schetst de Kafkaëske situaties die ontstaan wanneer burgers verdwalen in de steeds complexer wordende – ketens van – overheidsorganisaties. Besluitvormingsprocedures verlopen niet alleen steeds langzamer, maar op het moment dat er foute beslissingen worden genomen is het erg moeilijk voor burgers om daar iets tegen te doen, te meer omdat het voor hen lang niet altijd duidelijk is waar ze moeten aankloppen. Kleine fouten die doorwerken in het hele systeem krijgen enorme consequenties voor hen en kunnen hun leven behoorlijk overhoop gooien (zie ook de Jong et al., 2008).

3.5 Conclusie

In dit hoofdstuk is beschreven hoe traditionele op papier gebaseerde registraties waarop de overheidsbureaucratie is gebouwd via digitale kaartenbakken evolueren richting digitale identiteiten. De op individuen betrekking hebbende digitale dataverzamelingen betreffen niet langer een beperkte hoeveelheid attributen en feiten, maar strekken zich meer en meer uit tot gedetailleerde overzichten over de identiteit van burgers op basis waarvan veel meer kan worden gedaan dan het geval was bij de meer eenvoudige registraties. De moderne digitale identiteiten kunnen functioneren als representaties van mensen van vlees en bloed. De inbreng van echte burgers is steeds minder noodzakelijk om beslissingen over hen te nemen. De overheid kan uit de voeten met de digitale burger.

In dit hoofdstuk hebben we ons vooralsnog voornamelijk beperkt tot gegevensverzamelingen zoals die door een enkele organisatie worden bijgehouden. Hoewel we ook hier al kunnen zien dat door het rijker worden van de representaties beslissingen over individuele burgers kunnen worden genomen die verder rijken dan waarvoor de gegevens in strikte zin oorspronkelijk waren verzameld (denk aan het voorbeeld van de kinderbijslag), is er nog steeds sprake van een duidelijke band tussen doel en gebruik van de verzamelde gegevens.

In het volgende hoofdstuk zullen we laten zien dat er een ontwikkeling valt te verwachten, en op beperkte schaal al zichtbaar is, waarbij deze band losser is en misschien wel wordt losgelaten. Het gaat dan om identiteiten die worden geconstrueerd door verschillende deelidentiteiten met elkaar te verbinden: samengestelde identiteiten.

4. Samengestelde en gedeelde identiteiten

4.1 Inleiding

Identiteit is een complex begrip met verschillende gezichten afhankelijk van het gekozen perspectief dat verandert onder invloed van nieuwe technologieën. Identiteiten worden in toenemende mate gedigitaliseerd en leiden daarmee tot 'digital personae' (Clarke, 1994). Bovendien worden identiteiten steeds rijker, d.w.z. ze omvatten meer data dan voorheen, en geven een steeds indringender beeld van de gerepresenteerde. Tegelijkertijd ontstaat er een afstand tussen gerepresenteerde en diens identiteit, wanneer de laatste een eigen leven gaat leiden in netwerken en ketens. In dit hoofdstuk richten we ons op wat we noemen samengestelde en gedeelde identiteiten. Deze concepten komen voort uit tendensen naar digitalisering, data-intensiteit, abstractie en holisme.

4.2 Van enkelvoudige naar samengestelde identiteiten

Iedere uitvoeringsinstantie binnen de publieke sector onderhoudt ten behoeve van de uitvoering van het beleid administraties. Voor zover het beleid betrekking heeft op burgers betreffen deze administraties dus databanken waarin gegevens over burger worden bijgehouden. In de woorden van Clarke (1994) onderhouden overheidsorganen ieder voor zich de 'imposed digital personae' noodzakelijk voor de uitoefening van hun taken en verantwoordelijkheden. Deze deelidentiteiten vormden een weergave van de burger voor zover relevant voor de specifieke organisatorische context waarbinnen deze werd gebruikt. Met het ontstaan van de moderne samenleving waarin een steeds grotere nadruk is komen te liggen op informatie, controle en maakbaarheid van de samenleving is het landschap van het openbaar bestuur sterk veranderd. Mettertijd zijn overheidsorganisaties bijvoorbeeld steeds meer gaan samenwerken om gemeenschappelijke beleidsdoelen beter te kunnen realiseren. Deze samenwerking betekent onder andere dat tussen hen op steeds grotere schaal informatie wordt uitgewisseld. We spreken dan van keteninformatisering, waarbij de betrokken organisaties de autonome kralen in de informatieketting zijn. Grijpink (2007) definieert het begrip 'keteninformatisering' als volgt:

> *Keteninformatisering beoogt ontwikkeling van ketenspecifieke informatie-infrastructuren nodig voor geautomatiseerde communicatie in een keten.*

Keteninformatisering vereist dat gegevens van de verschillende betrokken instanties worden gestandaardiseerd en geïntegreerd. Standaardisatie en integratie symboliseren vaak twee kanten van dezelfde medaille, aangezien de eerste vaak met zich brengt dat per saldo de data-intensiteit in een organisatie groeit. Niet alleen worden de definities voor datasets samengevoegd, maar tevens kan het zijn dat deze worden uitgebreid. Een voorbeeld is de Basis Data Set die wordt gebruikt bij het Elektronisch Kind Dossier. Naast de gegevens die reeds konden worden genoteerd in papieren dossiers, kan nu nieuwe data waarvan de kinderartsen het wenselijk achten dat deze kunnen worden geregistreerd in het digitale dossier, worden ingevoerd. Belangrijk is te onderkennen dat dit samenwerken niet zozeer een uitwisseling van gegevens (over individuen) betreft, maar dat er kwalitatief iets verandert. Uiteraard gaat het op een bepaald technisch niveau over het uitwisselen van gegevens, maar de gegevens aan de bron en bij de bestemming hebben in hun samenhang een bepaalde betekenis; ze vertegenwoordigen deelidentiteiten van burgers. Iedere deelnemer in de keten beschikt reeds over een bepaald beeld van de relevante individuen, ze beschikken elk over een voor hun functie relevante deelidentiteit van hun klanten of cliënten. Deze deelidentiteit bestaat uit de manier waarop de burger zich binnen het betreffende beleidsterrein presenteert (haar 'projected persona') en het door de overheidsinstantie geconstrueerde relevante beeld (het 'imposed persona').

Als een gevolg van keteninformatisering worden de afzonderlijke deelidentiteiten bij organisaties samengevoegd tot rijkere (deel)identiteiten of steeds completere identiteiten van de burger. De aldus ontstane identiteit zegt, per definitie, meer over het individu dan de constituerende onderdelen afzonderlijk. Het geheel representeert een rijker beeld van het individu. Dit is wat we bedoelen met samengestelde identiteiten; een samengestelde identiteit is opgebouwd door het samenvoegen van twee of meer afzonderlijke deelidentiteiten van één en hetzelfde individu.[10] Interconnectiviteit is in onze definitie dus een een belangrijke *conditio sine qua non* om te kunnen spreken van samengestelde identiteiten.

Op basis van het voorgaande komen we tot de volgende definitie van samengestelde identiteiten:

> *Een samengestelde digitale identiteit is een digitale identiteit die is uitgebouwd door van twee of meer onafhankelijke entiteiten afkomstige digitale deelidentiteiten samen te voegen.*

Het samenvoegen van deelidentiteiten vereist dat is vast te stellen welke deelidentiteiten betrekking hebben op een bepaald individu. In dit verband is het handig om aan te sluiten bij terminologie van Roger Clarke.

---

10 Taalkundig kan ook van samengestelde identiteiten worden gesproken wanneer slechts sprake is van een enkelvoudige constructie van een digitale identiteit omdat deze immers ook wordt samensgesteld uit verschillende gegevens. Het gaat ons echter niet om het samenstellen van een identiteit uit verschillende attributen maar om het samenstellen van een identiteit uit verschillende deelidentiteiten die elk uit verschillende attributen bestaan.

> *"Individual people perform various social, economic and political functions, in roles such as citizen, consumer, sole trader, and member of partnerships ... A person may present the same persona for every role, or different personae for each of them, or a few personae each of which is used in multiple contexts ... It is useful to have a term available that encompasses both identities and the entities that underlie them ... the term "(id)entity" is used for that purpose."(Clarke, 2003 zoals aangehaald in, Raab, 2009)*

Clarke (2003) onderscheidt tussen 'identity' en 'entity'. Hij beschouwt 'human identity' als een bepaalde representatie van van een 'human entity'. '*Identity*' verwijst daarmee naar een onderliggende (fysieke) '*entity*'. Clarke gebruikt het begrip '*(id)entity*' om de verbinding tussen 'identity' en de onderliggende 'entity' aan te duiden. '(Id)entifiers' zijn:

> *"[O]ne or more data-items concerning an (id)entity that are sufficient to distinguish it from other instances of the same class, and that can therefore be used to signify that (id)entity." (Clarke, 2003, p. 634)*

'Entifiers' duiden een 'entity' aan.

Om een samengestelde identiteit te construeren moet de '(id)entity' van een bepaalde 'entity' worden vastgesteld (om welk individu in de werkelijkheid het gaat) en vervolgens moet een vergelijking en koppeling van records bij de verschillende constituerende entiteiten plaatsvinden op basis van de verschillende door deze organisaties gehanteerde '(id)entifiers'. Dat is een niet triviale operatie omdat er verschillende manieren zijn om gegevensverzamelingen te ordenen en de indexen tot de datasets kunnen dus verschillen. Koppeling op basis van de naam (eventueel aangevuld met andere gegevens, zoals adres of geboortedatum) werkt in sommige gevallen maar doorgaans niet of gebrekkig. Namen worden verschillend opgeslagen (zeker wanneer daar diacrytische tekens in voorkomen), de naam van gehuwde vrouwen wijkt soms af van die van voor hun huwelijk, etc. Het is dan ook niet verwonderlijk dat er een roep is om unieke identificatienummers toe te kennen aan de geregistreerde personen.

Binnen de verschillende sectoren binnen het openbaar bestuur hebben verschillende unieke persoonsnummers bestaan, zoals het A-nummer in gemeentelijke basisregistraties, het SoFi nummer in het sociale zekerheids- en belastingdomein, student- en onderwijsnummers, etc. Uniformering naar één enkel nummer binnen de publieke sector maakt het mogelijk om de verschillende deelidentiteiten van een individu in de verschillende administraties te lokaliseren op basis van diens persoonsnummer. Als de deelidentiteiten zijn te vinden, zijn ze ook te koppelen en combineren tot een samengestelde identiteit. Deze unieke '(id) entifier' is in Nederland het BurgerServiceNummer.

Daarnaast speelt het systeem van basisregistraties een belangrijke rol in het samenstellen van digitale identiteiten van burgers. De registraties omvatten zogezegd de basisdata voor de identiteitsconstructie. Ze functioneren als 'single

sources of truth' (Raab, 2009, p. 239) en vormen de authentieke bronnen van identiteitsgegevens die door overheidsorganen moeten worden geconsulteerd. Ideeën achter het stelsel van basisregistraties zijn onder andere dat het delen van persoonsgegevens van burgers een lastenverlichting voor zowel burgers als overheid betekent en bijdraagt aan het handhaven van de openbare orde en veiligheid en fraudebestrijding. Een voorbeeld van een basisregistratie is de Gemeentelijke Basis Administratie (GBA) die onder meer de volgende gegevens bevat: naam, woonadres, geslacht, Burger Service Nummer en administratienummer. Het is de bedoeling dat de 'imposed digital persona' die een overheidsorgaan heeft van een burger zowel wordt samengesteld uit data die deze organisatie zelf verzamelt en genereert als ook door verwijzingen naar gegevens die zijn geregistreerd in andere basisregistraties. De deelidentiteit die openbare scholen samenstellen uit het leerlingvolgsysteem kan bijvoorbeeld worden aangevuld met data uit een basisregistratie, waaronder het in de GBA geregistreerde woonadres van de scholier. De basisregistratie-identiteit kan worden beschouwd als de kern– of de basisidentiteit van iedere burger, waarop overheidsorganisaties kunnen voortbouwen. Dit gebeurt in het algemeen door het toevoegen van attributen (identiteits– of persoonsinformatie) door de betreffende instantie aan de kernidentiteit van burger, gegeven dat de specifieke context substantiëlere informatie over de burger vereist. In het voorbeeld van de openbare scholen valt te denken aan cijfers, absentiegegevens en gegevens over psycho-sociale problemen. Vanuit het perspectief van de organisatie gaat het dan om zogeheten functioneel relevante data (Zarsky, 2002, 2004), zoals bijvoorbeeld:

> *"[N]umber of children, religious confession, education, profession, creditworthiness, nationality, aspects confirming legal capacity or special attributes for scientific inquiries."*

4.3 Van samengestelde naar gedeelde identiteiten

Een gerelateerde ontwikkeling is het ontstaan van gedeelde identiteiten. Dit zijn digitale identiteiten waarbij digitale deelidentiteiten samensmelten met het doel om een compleet of op zijn minst completer beeld van de burger te creëren. Het kenmerkende aspect van gedeelde identiteiten is dat deze per definitie context-overschrijdend worden geconstrueerd door overheidsorganisaties. In eerder gebruikte voorbeeld van het onderwijsdomein (de burger in de rol van scholier) zou dit kunnen betekenen dat de 'imposed digital persona' wordt gekoppeld aan gegevens in het domein van de gezondheidszorg (burger in de rol van patiënt), de jeugdzorg (burger in de rol van probleemjongere) of justitie (burger in de rol van (potentiële) verdachte of crimineel). Dit kan om uiteenlopende redenen gebeuren, bijvoorbeeld om in brede zin ontwikkelingsproblemen van (risico–)jongeren of kindermishandeling te signaleren en aan te pakken. Door het over contexten heen delen en samenvoegen van data over burgers groeit de data-intensiteit en ontstaat een meer holistische representatie van burgers in de informatieketen. Gedeelde identiteiten ontstaan veelal door het koppelen of integreren van verschillende

databanken. Ook hier zijn unieke persoonsnummers, zoals het BSN in Nederland, van groot belang om de gedeelde identiteiten daadwerkelijk en betrekkelijk eenvoudig te kunnen construeren.

Het vervolg van ons betoog hanteert als definitie van het begrip 'gedeelde identiteit':

> *Een gedeelde identiteit is een digitale identiteit die is uitgebouwd door van twee of meer onafhankelijke entiteiten afkomstige digitale deelidentiteiten samen te voegen over verschillende beleidscontexten heen en die in de verschillende constituerende domeinen wordt gebruikt.*

Met andere woorden, de gedeelde identiteit is een context-overschrijdende samengestelde identiteit, waarbij met de term 'context' wordt gerefereerd aan onderscheiden beleidsdomeinen.

4.4 Van beleidskokers naar maatschappelijke ketens

Het antwoord op de vraag waarom de constructie van samengestelde en gedeelde identiteiten van belang is voor de overheid ligt tamelijk voor de hand. Traditioneel gezien bestaan er binnen het openbaar bestuur onderscheiden beleidskokers die – gebaseerd op eigen behoeften en vooronderstellingen – ieder voor zich een binnen hun realiteit passende representatie van de burger construeren. Overheidsorganisaties en -instanties *definiëren* de burger in hun beleidswereld, of zoals Raab het zegt in het licht van identity cards:

> *"[Y]ou are who we say you are, on the basis of facts registered and recorded in predetermined categories" (Raab, 2009, p. 239).*

Deze representatie is gekoppeld aan de verschillende rollen die de burger ten opzichte van de overheid vervuld, zoals uitkeringsgerechtigde, belastingbetaler, consument (bijvoorbeeld wanneer hij of zij producten van het Kadaster koopt), asielzoeker, student, inwoner van een gemeente, etc. Door een toenemende complexiteit van onze moderne maatschappij laten de sociale problemen waarvoor de overheid zich gesteld ziet zich evenwel steeds minder goed aanpakken binnen de grenzen van die verschillende beleidsdomeinen. Organisaties die opereren binnen een bepaald beleidsdomein zien slechts een deel van het plaatje, terwijl soms alleen een omvattender beeld kan leiden tot signalering of oplossing van complexe, domein-overschrijdende problemen. Het beeld van een organisatie over burgers in hun beleidsveld is daarmee in principe mogelijk slechts accuraat voorzover het betrekking heeft op relevante gegevens binnen het kader van hun beleidsopdracht. Het gevolg is dat ze niet of onvoldoende op de hoogte zijn van de urgentie van – maatschappelijke relevante – problemen met betrekking tot

individuele burgers. Een goed voorbeeld zijn de problemen in de jeugdzorg. [11] Zowel de huisarts als het schoolmaatschappelijk werk kan vermoedens hebben van kindermishandeling bij een patiënt respectievelijk scholier, maar zolang zij niet communiceren blijft een compleet beeld van de situatie op basis waarvan (tijdig) ingrijpen mogelijk wordt wellicht uit. Het koppelen van data(banken) en daarmee realiseren van samengestelde of gedeelde identiteiten wordt wel beschouwd als een noodzakelijke en onontkoombare ontwikkeling in het oplossen van de coördinatie-problemen als gevolg van de lappendeken aan organisaties en professionals die in complexe beleidsdomeinen moeten opereren. Prins (2009) merkt ten aanzien van de jeugdzorg op:

> *"Wat bij de tendens tot verbinden en koppelen opvalt, is dat een organisatorische eenheid als de school, het consultatiebureau, of een Bureau Jeugdzorg steeds minder centraal komen te staan, en de focus steeds meer wordt verlegd naar het organiseren en handelen rondom* ***belangen, problemen, risico's*** *om te komen tot* ***hulp, zorg, bijsturing****." (p. 36)*

We kunnen het beeld breder trekken naar de overheid meer in het algemeen. Een ander voorbeeld is de lokale dienstverleningsketen die ontstaat naar aanleiding van de Wet Maatschappelijke Ondersteuning (WMO). Het doel van de WMO is om ervoor te zorgen dat burgers blijven meetellen in de samenleving. Niet alleen gemeenten zijn betrokken bij de implementatie van deze wet, maar ook allerlei – publieke en private – ketenpartners, waaronder Centrum Indicatiestelling Zorg (CIZ), GGDs, thuiszorg-organisaties, MEE-organisaties en Stichting Welzijn Ouderen. Steeds vaker is dus niet langer de organisatie het uitgangspunt van beleid, besluiten en handelen, maar wordt er geageerd vanuit een sociaal (on) wenselijk geachte situatie, waarbij diverse betrokken partijen – ongeacht hun beleidsdomein, – aanhaken. De burger en diens probleem situatie komt meer en meer centraal te staan. Organisatiegrenzen vervagen daarmee en informatie vloeit vrijer tussen de verschillende entiteiten.

4.5 Focus op risico's, veiligheid en preventie

Het voorgaande is echter slechts een deel van het verhaal. We zien ook een ontwikkeling waarin de overheid meer en meer aandacht heeft voor maatschappelijke risico's, risico-management, veiligheid en preventie. Van handelen *ex post* vindt er een verschuiving plaats naar ingrijpen *ex ante*. Illustratief voor deze trend is het overheidsproject Veiligheid begint bij voorkomen.[12] Aldus de website, omvat het project Veiligheid begint bij Voorkomen vele maatregelen die een bijdrage moeten leveren aan het substantieel verminderen van criminaliteit en overlast in Nederland. Het project gaat uit van een integrale werkwijze, met acties van lokaal bestuur en de rijksoverheid, en van preventieve inspanningen in

11 Bekend in dit verband is de Rowena zaak. Zie bijvoorbeeld <http://www.dordt.nl/nieuws/dossiers/rowenarikkers>.

12 Zie: <http://www.veiligheidbegintbijvoorkomen.nl>.

combinatie met repressie. Het project bevat maatregelen op de thema's agressie en geweld, overlast en verloedering, georganiseerde criminaliteit, criminaliteit bedrijfsleven en persoonsgerichte aanpak.

Een groeiende focus op het voorkomen van individuele en maatschappelijke risico's betekent eveneens dat de behoefte aan context-overschrijdende data en deelidentiteiten toeneemt. Gegevens vormen namelijk de grondstof op basis waarvan in het risico-scenario waarschijnlijkheden worden berekend of nieuwe kennis kan worden gegenereerd. In het voorgaande hoofdstuk refereerden we al aan het ontstaan van persoonlijke of risico-profielen als speciale vormen van 'digital personae'. De profielen kunnen iets zeggen over de waarschijnlijkheid waarmee een burger een bepaalde – bijvoorbeeld als risico gekwalificeerde – gedraging zal vertonen. Bijvoorbeeld over de mate van (on)waarschijnlijkheid dat Ronald en Simone fraude zullen plegen met gemeenschapsmiddelen of een snelheidsovertreding begaan, maar ook zou hun kredietwaardigheid iets kunnen zeggen over de mate waarin de overheid hen kan vertrouwen.[13] Risicoprofielen zullen veelal samengestelde of gedeelde identiteiten zijn, maar wel met een bijzonder karakter. Deze profielen bestaan namelijk niet alleen uit feitelijke data, maar op basis van de attributen die iets zeggen over het individu en wellicht andere (bijvoorbeeld demografische) informatie die aan het individu kan worden gerelateerd worden uitspraken gedaan over (te verwachten) toekomstig handelen van het individu. Van het inschatten van risico's die het individu behelst, is het vervolgens een kleine stap naar categorisering en waardering van burgers op basis van hun risicoprofiel. Risicoprofilering kan op die manier verregaande sociale consequenties hebben. Dit is wat Lyon (2001) heeft aangeduid als 'social sorting'.

Ofschoon risico-profilering nog geen grote vlucht heeft genomen bij de Nederlandse overheid zien we toch al de eerste tekenen dat dit lijkt te veranderen. De discussies rond het Elektronisch KindDossier zijn hiervan een voorbeeld. Binnen de politie is ingezet op ontwikkelingen zoals 'nodale oriëntatie' (Projectgroep Visie op de politiefunctie, 2005)

> *"De nodale oriëntatie ('infrastructuurpolitie') leidt tot toezicht houden op de infrastructuur. Of beter, op de stromen van mensen, goederen, geld en informatie die zich over de infrastructuur verplaatsen. Daartoe controleert de politie op de knoop- punten van de netwerken (ringwegen rond steden, overslagpunten, havens, luchthavens) van uiteenlopende geografische schaal en van verschillende aard (stedelijk, interstedelijk, interstatelijk, virtueel). De controlefunctie is gericht op het opheffen van anonimiteit en onzichtbaarheid en het identificeren van 'kwaad' in de vorm van potentiële en actuele bedreigingen van de veiligheid. De controlefunctie is meer gericht op personen of groepen dan op delicten. Dat betekent dat de onderverdeling in specialismen (bijvoorbeeld voertuigveiligheid, alcohol in het verkeer, verkeersovertredingen) minder interessant wordt ten gunste van controles gericht op de breedte van het vakgebied. Naar verwachting zal de technologie hierbij een steeds belangrijker rol gaan spelen. Dit betreft vooral de*

13 Dit laatste is geen fictief voorbeeld; in het geval van de Engelse overheidswebsite Government Gateway voert het bedrijf Experian de online authenticatie van de burger uit door onder meer een 'trust score' te berekenen op basis van diens gegevens in een groot aantal publieke en private databases, waaronder databanken met gegevens over kredietwaardigheid van individuen, Taylor e.a. (2009).

high tech toepassingen, zoals catch scan-technieken waarbij waarnemingen en registraties van personen en voertuigen worden vergeleken met uiteenlopende databestanden (bijvoorbeeld openstaande boetes, gestolen voertuigen, vermiste kentekenplaten, bekende verdachten). Hierdoor wordt het mogelijk 'kwaad' te identificeren en een halt toe te roepen. Daarmee wordt ook voorkomen dat onverdachte personen onnodig in hun privacy worden aangetast." (Projectgroep Visie op de politiefunctie, 2005, p.90)

4.6 De schaduwkant van moderne identiteiten

De effecten van het ontstaan en vervolgens het gebruik van samengestelde of gedeelde identiteiten vallen in tweeën uiteen. Enerzijds bieden deze 'digital personae' kansen die er voorheen niet waren, doordat individuele behoeften en risico's over de grenzen van beleidsdomeinen heen kunnen worden geïdentificeerd en effectiever beantwoord door de overheid. Maar er kleven ook risico's aan deze holistische digitale identiteiten die verder gaan dan de risico's van het gebruik van meer beperkte 'digital personae'.

Veel is geschreven over de (privacy) risico's van gegevensbestanden bij de overheid (bijv. Anderson et al., 2009, Schermer en Wagemans, 2009, Vedder et al., 2007). Deze literatuur is onverminderd toepasselijk voor samengestelde identiteiten. Deze identiteiten zijn immers datasets. Doordat ze zijn opgebouwd uit deelidentiteiten uit verschillende contexten ontstaan echter ook een aantal specifieke problemen en risico's die we in deze paragraaf nader uitwerken. De risico's kunnen worden onderscheiden naar fundamentele en meer praktische problemen. Het onderscheid tussen de verschillende typen problemen is niet altijd even scherp, ze hangen sterk met elkaar samen.

Fundamenteel
Ondermijning van mogelijkheden tot contextscheiding
Decontextualisering
Vermindering van autonomie / verlies van controle
Ondermijning van mogelijkheden tot 'identity negotiation'
Stereotypering
Facilitering van identiteitsfraude
Praktisch
Foutieve koppelingen
Intransparante fouten

Tabel1 : Risico's van samengestelde en gedeelde identiteiten

4.6.1 Ondermijning van mogelijkheden tot contextscheiding

Een eerste bezwaar van samengestelde identiteiten is dat bij de constructie van een dergelijke identiteit per definitie informatie uit meerdere contexten wordt gecombineerd. Het beeld dat al dan niet bewust door het individu in de verschillende constituerende contexten is gepresenteerd met het oog op de regels, waarden en gebruiken binnen die specifieke contexten wordt daarmee samengevoegd zonder rekenschap te geven van de deelcontexten. De presentatie die een individu in een bepaalde context geeft en die bedoeld kan zijn om binnen die context te blijven wordt zichtbaar in een context waarover het individu geen controle heeft en het bestaan waarvan zij zich mogelijk zelfs niet bewust is. Hiermee wordt het individu dus tevens mogelijkheden ontnomen om een bepaalde rol te spelen binnen een bepaalde context, er bestaat immers een gereed risico dat identiteitsinformatie doorsijpelt naar andere contexten. Het feit dat een van de auteurs in zijn professionele hoedanigheid hoogleraar is kan de aanvraag tot een monumentensubsidie ter verbouwing van het woonhuis onzakelijk beïnvloeden (die zal wel een riant inkomen hebben en subsidie niet echt nodig hebben). Informatie over beroep en 'rang' is door het combineren van contexten mogelijk moeilijker te beperken tot de relevante contexten.

De tegenwerping dat het informatie over hetzelfde individu '(id)entity' betreft en dat het in de publieke sector gaat over feiten en dat deze derhalve zonder bezwaar kunnen worden samengevoegd is een simplificatie en onderschatting van het belang van deelcontexten. Meer informatie over een individu levert niet altijd een betere basis voor beslissingen op. Aangezien besluiten in de publieke sector gebaseerd moeten zijn op een wettelijke basis, is het regelgeving die voorschrijft welke rechtsgevolgen aan bepaalde omstandigheden moeten worden verbonden. Informatie die verder gaat dan deze noodzakelijkheidsvereisten kan de beslissingen onredelijk beïnvloeden. Het hoogleraarschap van een der auteurs kan zijn aanvraag tot een monumentensubsidie zoals gezegd onzakelijk beïnvloeden. Beroep is informatie die niet relevant mag zijn voor het oordeel over de aanvraag. Ware dat wel zo dan had het in de voorwaarden moeten zijn opgenomen.

Bovendien komt onze sociale identiteit onder druk doordat koppeling en uitwisseling van digitale identiteiten onze mogelijkheden sociale contexten te scheiden verkleint (Introna, 1997).

4.6.2 Decontextualisering

Verschillende auteurs stellen dat het samenvoegen en toegankelijk maken van digitale identiteiten buiten de contexten waarin deze zijn gecreëerd, risico's oplevert met betrekking tot de interpretatie van de resultaten doordat noodzakelijke context-informatie ontbreekt of de samengestelde digitale identiteiten inconsistente of onjuiste representaties van de betrokken opleveren (Clarke, 1994, p. 13, Gandy, 1993, Lyon, 2004, pp. 142-143, Solove, 2007b, p. 66, W.,

2001, pp. 21-27). Een partiële digital persona wordt geconstrueerd in concrete en redelijk afgebakende context en representeert het individu in die context. De data (attributen) waaruit deze persona bestaat moet voor een goed begrip binnen de kaders van die context worden uitgelegd door specialisten. Op het moment dat 'digital personae' uit verschillende contexten worden gecombineerd, kunnen er twee dingen gebeuren. Het beeld dat ontstaat biedt op relevante aspecten een verkeerde representatie van het individu, of het ontstane beeld wordt gebruikt zonder dat de representatie wordt begrepen omdat het interpretatiekader ontbreekt. In dit verband is het door Nissenbaum (2004) geïntroduceerde concept 'contextual integrity' relevant.[14]

> *"A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation. These contexts can be as sweepingly defined as, say, spheres of life such as education, politics, and the marketplace or as finely drawn as the conventional routines of visiting the dentist, attending a family wedding, or interviewing for a job. [...] Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices." (p. 119 -120)*

Nissenbaum verbindt het concept van 'contextual integrity' aan een tweetal normen voor het gebruiken van persoonsgegevens door actoren in een gegeven context: de normen van 'appropriateness' en die van 'flow or distribution'. De eerste soort schrijft voor welke data er een specifieke context mag of moet worden verstrekt door de burger. Zo zal in een medische context van ons mogen worden verwacht dat we de arts informeren over onze fysieke of geestelijke gesteldheid opdat een passende diagnose kan worden gesteld. Wanneer we een werkeloosheidsuitkering aanvragen is deze informatie niet relevant, maar in het geval van een arbeidsongeschiktheidsuitkering ligt dat weer anders. Het is duidelijk dat het per context sterk kan verschillen welke informatie passend is om uit te wisselen binnen de specifieke relaties in het licht van de taken en doelen die daar bestaan. De tweede soort normen stelt vast of contextuele normen worden gerespecteerd bij de uitwisseling van deelidentiteiten. Een voorbeeld van een dergelijke norm is het medisch beroepsgeheim (vertrouwelijkheid) in de relatie tussen patiënt en arts. Een norm waaraan bepaald weinig of niet wordt gerefereerd in beleidsvisies op een breed inzetbaar Elektronisch Kind Dossier, een dossier dat in aanleg toch een medisch dossier is. Dit voorbeeld wordt in hoofdstuk 5 verder uitgewerkt. Als contexten in informationele zin in elkaar over gaan lopen dan gaat dit ten koste van de contextuele integriteit en daarmee de privacy van de burger. Er dienen derhalve zwaarwegende gronden te zijn om de situatie te veranderen. Nissenbaum schrijft hierover:

---

14 Nissenbaum baseert zich op Michael Walzer's befaamde 'Spheres of Justice' (1983).

"[T]he requirement of contextual integrity sets up a presumption in favor of the status quo. [...] A presumption in favor of the status quo for informational norms means we initially resist breaches, suspicious that they occasion injustice or even tyranny. We take the stance that the entrenched normative framework represents a settled rationale for a certain context that we ought to protect unless powerful reasons support change. The settled rationale of any given context may have long historical roots and serve important cultural, social, and personal ends. [...] A presumption in favor of status quo does not, however, rule out the possibility of a successful challenge where adequate reasons exist. Resolving these contested cases calls for reliable means of evaluating the relative moral standing of entrenched norms and the novel practices that breach or threaten them. Specifically, I propose that entrenched norms be compared with novel practices that breach or threaten them, and judged worth preserving, or not, in terms of how well they promote not only values and goods internal to a given context, but also fundamental social, political, and moral values."

Het delen van identiteiten over contexten heen zou geen "louter" organisatorisch-technische beslissing mogen zijn, maar dient weloverwogen en duidelijk gemotiveerd plaats te vinden. Het vraagt om argumentatie hoe een dergelijke verandering in administratieve praktijken zich verhoudt tot het waarborgen van fundamentele waarden alsmede rechten en vrijheden van individuele burgers.

De effecten van ondermijning van contextuele integriteit komen naar voren in de volgende subparagrafen.

4.6.3 Vermindering autonomie en verlies controle

De ontwikkeling van de persoonlijke identiteit of – in andere woorden – persoonlijke autonomie is een van de fundamentele, in onze Westerse samenleving erkende vrijheid van individuen. Ofschoon het recht als zodanig niet is te vinden in onze Grondwet, mag worden aangenomen dat het als onderdeel van het waarborgen van de menselijke waardigheid schuilgaat in onder meer de vrijheid van meningsuiting, het recht op een persoonlijke levenssfeer en het recht op lichamelijke integriteit (Van der Hof et al, 2009).

Eerder hebben we laten zien dat de identiteit van mensen wordt gevormd in interactie met anderen en dat het daarbij relevant is om vanuit een oogpunt van zelfontplooiing de vrijheid te hebben om in verschillende contexten, rollen en posities te experimenteren en te spelen met onze identiteit en aldus een specifiek beeld van onszelf neer te zetten. Op het moment dat administratieve systemen steeds holistischer identiteiten van burgers creëren door het samenvoegen en delen van deelidentiteiten over contexten heen kan dat ten koste gaan van onze persoonlijke autonomie. Onze identiteit wordt voor ons ontwikkeld op basis van een steeds uitbreidende data-set zonder dat we daar zelf nog veel invloed op hebben. Niet op het moment van identiteitsconstructie, noch op een later moment. Vervolgens vormt deze geconstrueerde identiteit de basis voor al dan niet geautomatiseerde overheidsbeslissingen met min of meer vergaande consequenties voor ons leven. Eerder hebben we deze ontkoppeling van

representatie en individu aangeduid met het begrip geabstraheerde identiteiten, waarmee we refereren aan digital persona die via unieke 'identifiers', bijvoorbeeld een persoonsnummer, verwijzen naar ons, maar feitelijk los zijn komen te staan van de persoon van vlees en bloed die we zijn. Behalve dat digital personae onze autonomie in zelfrepresentatie ondermijnen, betekent het feit dat ze een eigen leven leiden in de overheidsbureaucratie tevens dat we er niet of nauwelijks controle over hebben. Veelal is voor de burger niet duidelijk hoe gedeelde en samengestelde digital persona worden opgebouwd, noch hoe ze worden gebruikt door de overheid (en eventueel daarbuiten). Alarmerend wordt het, wanneer fouten in identiteitsconstructie niet of onvoldoende kunnen worden rechtgezet.

4.6.4 Ondermijning van de mogelijkheden tot 'identity negotiation'

Het gebruiken van samengestelde en gedeelde identiteiten kan ertoe leiden dat de mogelijkheden tot 'negotiation of identity' (Raab 2009, p. 231) worden ondermijnd. Het begrip 'identity negotiation' is nauw verbonden met het symbolisch interactionisme van eerdergenoemde sociologen zoals Goffman, Mead en Cooley. Het concept verwijst naar de wijzen waarop personen overeenstemming bereiken over wie wie is of welke rol iemand heeft in een bepaalde context of relatie. Swann (2005) omschrijft dit als volgt:

> *"Identity negotiation refers to the processes through which perceivers and targets come to agreements regarding the identities that targets are to assume in the interaction. " (p. 69).*

Dit is een interactief en dynamisch proces. Na verloop van de tijd kan het noodzakelijk zijn dat opnieuw overeenstemming over de inhoud van identiteiten plaatsvindt. Op die manier wordt gewaarborgd dat het actief gebruikte digital persona blijvend aansluit bij de realiteit. In psychologisch en sociologisch perspectief zouden we spreken van processen van zelf-verificatie; in de context van 'public administration' hebben we het meer algemeen over verificatieprocessen aangezien – vanuit haar rol bezien – de overheid cruciale actor is in het proces. De overheid heeft onmiskenbare belangen bij en jegens de burger bijzondere verantwoordelijkheden voor zorgvuldige en accurate identiteitsconstructie en -verificatie. Dat neemt niet weg dat 'user-centric' mechanismen denkbaar zijn, waarin de burger zelf grotere controle heeft over zijn of haar identiteitsconstructie in relaties met de overheid (Van der Hof et al, p. 62).

Wanneer samengestelde en gedeelde digital personae een eigen leven gaan leiden zonder dat op gestelde momenten rekenschap wordt gegeven van de correctheid van de digitale representaties door terugkoppeling met individuele burgers is er een gerede kans dat onverwachte of foutieve beslissingen volgen. Van der Hof en Keymolen (2010) hebben het in dit verband over 'identities turned to stone':

> *"Thinking about identity as an evolving network of various relational roles, there is no solid property or such a thing as a "core self". A person is dynamic and identity*

will undergo changes over time. A profile is a representation of a person at a specific moment in time and cannot capture all these dynamics. The possibility exists that this profiled identity turns to stone in the system and does no longer sufficiently represent the person it belongs to. [...] Because of the dynamics of personal identities, individuals always escape a full representation." (p. 12)

Door ervoor te zorgen dat de burger niet volledig verdwijnt uit het verificatieproces of – andersom geredeneerd – hem daarin een uitdrukkelijke plaats te geven, kan wellicht worden voorkomen dat gedeelde en samengestelde digital persona te ver van diens persoon af komen te staan. Op zijn minst zou een zo adequaat mogelijke representativiteit moeten worden verzekerd.

4.6.5 Stereotypering

Eerder gaven we aan dat (risico)profilering een bijzondere vorm van samengestelde of gedeelde identiteiten oplevert, waarmee een soort van kansberekening van te verwachten risico's ten aanzien van groepen of individuele personen kan worden gemaakt. Het idee is dat de overheid vervolgens gerichter aandacht kan besteden aan die burgers die – potentieel – (de grootste) sociale of economische risico's vormen in onze samenleving en daarmee wellicht risico's kan voorkomen. Tegelijkertijd gaat profilering noodzakelijkerwijs gepaard met een proces van generalisatie en categorisering om complexe situaties terug te brengen tot behapbare proporties en algemene standaarden (Schauer, 2003). Categorisering in algemene zin gebeurt ook door de overheid:

"Beleid is vaak gericht op bepaalde categorieën burgers: burgers met minderjarige kinderen, kinderen zelf, mensen met een ziekte of met in een bepaald opzicht een handicap, burgers zonder baan en inkomen, enzovoort. Categoriseren is reduceren. Beleid maken berust vaak op het 'vangen' van bepaalde groepen burgers in wettelijke beleidscategorieën. De burger wordt zo gereduceerd tot een bepaalde groep." (Nationale Ombudsman, 2009, p. 20)

Dit proces wordt ook wel aangeduid met de term 'stereotypering'. Stereotypering heeft echter ook een schaduwkant, aangezien het kan leiden tot ongerechtvaardigde vooroordelen en discriminatie. Zelfs als statistisch gezien blijkt dat burgers die op op postcode 1234 AB woonachtig zijn een grotere kans geven op uitkeringsfraude, dan betekent dit nog niet dat daarmee gerechtvaardigd is om iedere uitkeringsgerechtigde met die postcode preventief als fraudeur te bestempelen tot het tegendeel is bewezen. Hier betreden we het terrein van het *presumptio innocentia*: de burger is onschuldig zolang het tegendeel niet is bewezen.

In dit geval wordt ook wel gesproken van 'stigmatised identities' (Van der Hof, Keymolen, 2010) waarmee wordt verwezen naar het gevaar van ongerechtvaardigde bevooroordeling. 'Stigmatised identities' kunnen leiden tot ongewilde of onredelijke in- en uitsluiting van overheidsdiensten en daarmee tot

inbreuk op fundamentele waarden die de overheid dient te waarborgen. Uiteindelijk zal op de een of andere manier de mens achter de digital persona of het profiel zichtbaar moeten blijven om tot een goede beoordeling in individuele situaties te komen.

4.6.6 Faciliteren identiteitsfraude

Digitalisering van informatieprocessen draagt bij aan het ontstaan van nieuwe kwetsbaarheden. Een van die kwetsbaarheden is wat we noemen 'identiteitsfraude' of 'identiteitsdiefstal'. Identiteitsfraude en identiteitsdiefstal doen zich in verschillende vormen voor, maar een algemeen kenmerk is wel dat andermans persoonlijke gegevens of identiteiten worden misbruikt voor enige vorm van persoonlijk gewin. Koops et al (2008) beschrijven de ontwikkelingen die tot dit soort criminele activiteiten leiden als volgt:

> *"Face-to-face transactions are replaced by human-to-machine interactions. Machines represent identities by bits and bytes that are relatively easily obtainable by others. Identifiers – the keys to our digital identities, often numbers or usernames – together with a secret (PINs, passwords etc.) unlock access to financial services (e.g., creditcard transactions) or allow services to be obtained (e.g., social-welfare benefits) and so forth. [...] What completes the intuitive explanation of the growth of identity-related crimes is the opacity of the processing of personal data and the relative inexperience of both users and online service providers in preventing and handling (new) kinds of attacks on personal data." (p. 2)*

Deze omschrijving bevat ingrediënten (digitalisering, gebruik van unieke 'identifiers', ondoorzichtige informatieprocessen) die ook in het geval van samengestelde en gedeelde identiteiten aanleiding tot zorg zijn in het licht van identiteitsfraude. Eerder hebben we erop gewezen dat het BurgerServiceNummer een belangrijke rol heeft in het aan elkaar knopen van deelidentiteiten over contexten heen (vgl. Grijpink, 2006, Prins en Meulen, 2006). Het "openstellen" van de publieke sector kan deze gevaren verder vergroten, omdat hiermee de personenkring met toegang tot de 'identifiers' wordt uitgebreid. Dat identiteitsfraude geen theoretisch probleem is in informatieketens blijkt uit het Jaarrapport 2008 van de Nationale Ombudsman (2009), onduidelijk is vooralsnog wel hoe groot het probleem is. Over de eerste helft van 2009 heeft het Centraal Meldpunt IDfraude 97 meldingen ontvangen, waarvan 59 als verdacht zijn gekwalificeerd. Het verdient opmerking dat het Meldpunt slechts een beperkte capaciteit heeft en zich daarom niet sterk profileert, zodat het werkelijke aantal verdachte gevallen mogelijkerwijs hoger ligt.

4.6.7 Fouten door koppeling

In ieder informatiesysteem kunnen ongerechtigheden kruipen, bijvoorbeeld doordat er iets mis gaat in de data-invoer of doordat informatieprocessen als gevolg van technisch falen dan wel onzorgvuldig of kwaadwillig handelen gecompromitteerd raken. Keten-informatisering en de groeiende data-intensiteit binnen de overheid vergroten de risico's voor datakwaliteit en wakkeren digitale kwetsbaarheden aan.[15]

Er kan ten eerste van alles misgaan in het technisch-organisatorische proces waarin de verschillende informatiesystemen worden verbonden en afspraken moeten worden gemaakt over taken en verantwoordelijkheden van de deelnemende partijen. Door koppeling worden bovendien verschillende autonome schakels met kenmerkende eigenheden verbonden. Organisatorische eenheden gebruiken een eigen taal, waarbinnen begrippen specifieke, niet zelden door wet– en regelgeving voorgeschreven definities kennen. Het begrip 'inkomen' kent bijvoorbeeld bijzondere betekenissen al naar gelang de context waarin we ons bevinden. Ook in technische zin zal er tussen systemen moeten worden vertaald (conversie) als er verschillende software en standaarden worden gebruikt. Wanneer de vertaling op semantisch en syntactisch niveau niet goed gebeurt, dan kunnen daardoor eveneens fouten ontstaan.

Verder is vaak onduidelijk wie in de keten verantwoordelijkheid draagt voor eenmaal ontstane fouten, waardoor deze blijven rondzingen in de keten. Het Jaarrapport 2008 van de Nationale Ombudsman merkt hierover op:

> *"De burger raakt verstrikt in de ketens en het is voor de burger moeilijk of zelfs onmogelijk om daar uit te komen. Verschillende overheden of zelfs onderdelen van hun organisaties verwijzen naar elkaar. Als er iets mis is gegaan, is het moeilijk om de vinger op de zwakke plek te leggen. Het lijkt of iedereen maar voor een klein deel verantwoordelijk is en dus niemand direct aangesproken kan worden." (Ombudsman, 2009)*

Onjuiste gegevens die doorwerken in de keten blijken in de praktijk een groot probleem. Een kleine fout kan verregaande consequenties hebben wanneer het zich ongecorrigeerd verspreid. Daar komt bij dat data toch al op veel bredere schaal en eenvoudiger beschikbaar is in gekoppelde systemen. Veelal zal die data door door de hergebruikers niet eerst op juistheid worden gecontroleerd (Ombudsman, 2009).

Om datakwaliteit – en daarmee de kwaliteit van gedeelde en samengestelde digital persona – te bevorderen zijn in het stelsel van basisregistraties zijn als stelregels verplicht gebruik en een terugmeldplicht ingevoerd. Overheidsinstanties zijn verplicht om gebruik te maken van authentieke registraties en moeten bij twijfel over de juistheid van data melding doen bij de houder van de betreffende

[15] Tegelijkertijd erkennen we dat door het koppeling van bestanden juist ook fouten aan het licht kunnen komen, maar in deze paragraaf ligt de nadruk op de risico's.

basisregistratie. Wanneer sprake is van een keten van data-afnemers is voor betrokkenen echter niet altijd helder op wie de terugmeldplicht rust (van der Hof et al., 2008). De Nationale Ombudsman (2009) hekelt bovendien de rigiditeit van het systeem dat tot vertragingen in datacorrectie kan leiden. Daarnaast kan de burger gebruik maken van zijn correctierecht, maar dan zal hij wel moeten weten bij wie hij terecht kan. Dat is – zo zagen we net – vaak juist een probleem. Bovendien loopt hij steeds achter de feiten aan.

4.6.8 Intransparante fouten

Eerder hebben we vastgesteld dat overheid een steeds completer beeld krijgt van de burger door het samenvoegen en delen van deelidentiteiten. Keymolen (2007) heeft het over onzichtbare zichtbaarheid. De burger worden voor de overheid steeds transparanter maar op een wijze die voor de burger zelf volkomen intransparant is. Het werk en de organisatie van de overheid worden steeds complexer en als gevolg daarvan worden ook informatieprocessen binnen de overheid (de werking van de mid– en de backoffice) ingewikkeld. Vaak zijn de werkwijzen binnen de overheid niet of nauwelijks meer te doorzien voor de burger. Het is niet verrassend dat in deze ontwikkeling fouten die worden gemaakt intransparant kunnen zijn voor de burger. Niet alleen neemt dus de kans op fouten toe door koppeling van databanken, maar tegelijkertijd vermindert de zichtbaarheid van welke fouten, waar, hoe en door wie worden gemaakt. In de vorige paragraaf gaven we al aan dat er inmiddels zoveel verschillende partijen betrokken zijn in beleidsdomeinen of gegroepeerd rondom specifieke maatschappelijke vraagstukken dat het het voor de burger lastig, zo niet onmogelijk, is om vast te stellen wie er op fouten kan worden aangesproken. Daarnaast kan het voor de burger volkomen onduidelijk zijn *dat* er iets mis gaat in zijn "dossier". Dit is bijvoorbeeld het geval wanneer hij met volkomen onverwachte overheidsbeslissingen, zoals ten onrechte opgelegde boetes, rekeningen voor niet ontvangen zorg en een onterechte bestempeling tot kindermishandelaar, wordt geconfronteerd zonder helder inzicht te hebben in hoe deze precies tot stand zijn gekomen. Los van het feit dat intransparantie van de overheid en de fouten die zij maakt de burger in een zeer lastige positie kunnen brengen, is 'system opacity' bovendien een voedingsbodem voor identiteitsfraude of -diefstal.

4.7 Conclusie

Als gevolg van een toenemende interconnectiviteit binnen het openbaar bestuur ontstaan steeds rijkere digitale identiteiten van burgers. Bijzondere vormen zijn samengestelde en gedeelde identiteiten. In het geval van samengestelde identiteiten worden digitale identiteiten uitgebouwd door van twee of meer onafhankelijke entiteiten deelidentiteiten samen te voegen. Gedeelde identiteiten gaan een stap verder doordat in dat geval het samenvoegen van de digitale deelidentiteiten gebeurt over verschillende beleidscontexten heen en de aldus gecreëerde informatie wordt gebruikt in de verschillende beleidscontexten. Het doel is hier om complete identiteiten van burgers te creëren teneinde een

beleidsdomein overstijgende aanpak van sociale problemen mogelijk te maken. De constructie van samengestelde en gedeelde identiteiten is geen triviale operatie, omdat gegevensverzamelingen uit verschillende contexten uiteenlopend zijn vormgegeven. Unieke persoonsnummers en authentieke bronnen vormen onmisbare instrumenten om deze identiteiten zo effectief en efficiënt mogelijk te maken en te gebruiken.

Voor de overheid zijn samengestelde en gedeelde identiteiten belangrijk om het hoofd te kunnen bieden aan ingewikkelde beleidsvraagstukken waarvoor ze zich gesteld in een steeds complexer wordende samenleving. In toenemende wordt er geageerd vanuit sociaal onwenselijk geachte situaties ongeacht of daar diverse beleidsdomeinen en instanties betrokken zijn. Daarnaast is de overheid meer en meer gericht op het inschatten en voorkomen van maatschappelijke risico's, waardoor de behoefte aan context-overschrijdende digitale data en identiteiten groeit. Risicoprofilering is een voorbeeld van een relevante ontwikkeling in dit verband.

Ondanks de kansen die samengestelde en gedeelde identiteiten voor een effectief overheidsbeleid wellicht bieden, heeft de ontwikkeling van moderne burgeridentiteiten ook schaduwkanten. In dit hoofdstuk hebben we een onderscheid gemaakt tussen fundamentele en praktische risico's. In de eerste categorie vallen de volgende risico's: ondermijning van mogelijkheden tot contextscheiding, decontextualisering, vermindering van autonomie en verlies van controle, ondermijning van 'identity negotiation', stereotypering en faciliteren van identiteitsfraude. In de tweede categorie zijn wij fouten door koppeling en intransparante fouten. Al deze risico's zijn in dit hoofdstuk verder uitgewerkt en leiden tot de conclusie dat zowel de constructie als het gebruik van samengestelde en gedeelde identiteiten grote zorgvuldigheid vereisen maar ook inzicht in – potentiële – negatieve externaliteiten van veranderingen in persoonsinformatiebeleid en de mogelijkheden om ongewenste effecten te vermijden dan wel recht te trekken.

5. Praktijkvoorbeeld: het EKD

5.1 Inleiding

In dit onderzoek is gezocht naar voorbeelden in de publieke sector waarin sprake is van gedeelde en samengestelde identiteiten of plannen bestaan die tot de constructie van deze identiteiten leiden. Tijdens het onderzoek is gebleken dat voorbeelden lastig te vinden zijn, waarschijnlijk omdat de overheid nog niet zo ver is. Een voorbeeld is 'intelligence led policing'. Ofschoon de wil om volgens dit concept te gaan werken binnen de Nederlandse politie wordt aangekondigd in beleidsdocumenten, is tegelijkertijd duidelijk dat er nog aanzienlijke technisch-organisatorische barrières moeten worden overwonnen alvorens een start kan worden gemaakt met de plannen (van der Hof, Leenes en Fennell, 2009). Desalniettemin is er in ieder geval één uitzondering waar al wel een tendens naar het construeren van samengestelde en gedeelde identiteiten kan worden ontwaard: het elektronische kind dossier (hierna: EKD). Hierna wordt ingegaan op wat het EKD behelst en welke ontwikkelingen in dat verband leiden tot deze moderne identiteitsconstructies.

In het onderzoek hebben we verder geprobeerd om te achterhalen welke ervaringen burgers hebben met digitale dossiervorming bij de overheid, waarbij met name is gezocht naar situaties waarin de overheid gebruik maakt van gedeelde en samengestelde identiteiten van burgers. Dit deel van het onderzoek omvatte diverse methoden. Ten eerste zijn burgers op basis van een advertentie in enkele landelijke dagbladen uitgenodigd een online vragenlijst (zie bijlage) in te vullen. Het aantal reacties daarop was zeer gering. Verder is er contact gezocht met het Medlpunt Identiteitsfraude en Lastvandeoverheid.nl[16] met de vraag of zij cases hebben die wijzen op het gebruik van samengestelde en gedeelde identiteiten en inzicht geven in de ervaringen van overheid en burger met de constructie en het gebruik van deze identiteiten. Dit leverde vanuit het oogpunt van dit onderzoek evenmin relevante gevallen op. In het eerste geval – de online vragenlijst – was de kans op een grote(re) respons in verband met de gekozen methode klein. De methode is afhankelijk van de kans dat burgers daadwerkelijk kennisnemen van de advertentie en vervolgens de wil hebben en de moeite nemen om te reageren indien zij een relevante situatie kunnen melden. Voor de tegenvallende resultaten van de online vragenlijst en zoekopdracht bij overheidsinstanties kunnen verschillende oorzaken worden aangedragen. Samengestelde en gedeelde identiteiten lijken vooralsnog nauwelijks te worden gebruikt binnen de Nederlandse overheid. Het zijn bovendien tamelijk complexe concepten die lastig zijn uit te leggen en wel worden verwisseld met andere concepten (zoals gegevenskoppeling). Ook dit kan een rol hebben gespeeld bij het vinden van

16 Beide instanties ressorteren onder het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

relevante cases. Wanneer de onderzoekers zelf toegang zouden hebben tot relevante databestanden zouden mogelijk relevante voorbeelden zijn gevonden. De onderzoeker konden, uiteraard, niet grasduinen in de overheidsinformatiesystemen om zelf geschikte voorbeelden te zoeken. Voor relevante casus zijn ze derhalve afhankelijk van wat informanten aandragen, zowel bij relevante (overheids)instanties als door burgers. Wanneer deze met een 'verkeerd' perspectief op zoek gaan komen mogelijk relevante gevallen niet boven water. De gekozen methoden zijn daardoor wellicht minder geschikt voor het doel dat we met het onderzoek hadden. De precieze redenen zijn niet duidelijk maar het heeft ertoe geleid dat het 'empirische' deel van ons onderzoek zonder noemenswaardig resultaat is gebleven en we hier slechts het praktijkvoorbeeld van het EKD zullen toelichten.

5.2 Het EKD: Van enkelvoudige naar gedeelde identiteiten

De ontwikkeling van het EKD is begonnen als digitalisering van de jeugdgezondheidszorg (JGZ). In de loop van 2010 moeten de papieren dossiers in de JGZ zijn omgezet in digitale bestanden. Deze verplichting volgt uit de Wet publieke gezondheid (Stb. 2008, 460) en betreft de dossiers van alle kinderen in de leeftijd 0 – 19 jaar die het consultatiebureau of de schoolarts bezoeken. Deze dossiers bevatten informatie over de fysieke, cognitieve en psycho-sociale ontwikkeling van het kind en diens sociale situatie (familie, vrienden, school, enzovoorts).

Tot zover lijkt deze ontwikkeling niet veel meer te behelzen dan een digitalisering van werkprocessen zoals die vanuit een oogpunt van efficiëntie en effectiviteit overheidsbreed plaatsvindt. De op papier aanwezige identiteitsinformatie van kinderen en ouders wordt omgezet in digitale datasets, ofwel digital persona. Deels zijn deze digital personal 'projected' – namelijk voor zover ouders bepaalde informatie verstrekken en aldus een beeld van hun kind neerzetten – maar deels ook 'imposed' omdat deze tevens eigen observaties van de kinderarts of verpleegkunde over de situatie van het kind bevatten. Beide vormen lopen hier dus in elkaar over.

Binnen de JGZ wordt een verbreding van het EKD voorzien door ook anderen te betrekken in de dataverzameling en wellicht het -gebruik. Op de korte termijn is het de bedoeling om de digitale identiteiten in het systeem uit breiden met prenatale data. Op de wat langere termijn is voorzien in een koppelijk tussen EKD en EPD, waardoor bijvoorbeeld huisartsen toegang krijgen.

In aanzet blijft het EKD dan een JGZ-dossier. Ofschoon binnen de JGZ verschillende professionals en organisaties betrokken zijn bij een kind, is de context waarbinnen de dataset wordt geconstrueerd en gebruikt redelijk afgebakend. Zo op het eerste gezicht is er dus sprake van enkelvoudige identiteiten die nu worden gedigitaliseerd. Het verhaal gaat echter verder. De functionaliteit en toegankelijkheid zijn namelijk punten van discussie en inmiddels zijn er regio's in Nederland die vinden dat het EKD niet slechts een medisch maar een jeugdzorg-

dossier in brede zin moet zijn. De 'digital personae' in het EKD zijn relevant buiten de JGZ voor o.a. maatschappelijk werk, scholen of zelfs de politie.

Twee uitgangspunten zijn in dit denken belangrijk. Ten eerste kampt de jeugdzorg met grote problemen. Gebrek aan coördinatie tussen jeugdzorg-organisaties en -professionals leidt tot ertoe dat kinderen met problemen adequate hulp ontberen. Een van de maatregelen om het tij te keren is het verbeteren van de informatie-uitwisseling om misstanden tijdig te signaleren en erger te voorkomen. Het uitbouwen van het JGZ-EKD naar een EKD voor de jeugdzorg in het algemeen kan daaraan een belangrijke bijdrage leveren, zo is de gedachte. In deze visie moet het EKD een holistisch beeld van kinderen genereren door het bijeenbrengen van alle data die in de jeugdzorg over individuele kinderen wordt verzameld. Ten tweede past deze beleidsontwikkeling in een trend waarin de 'risicojongere' een steeds centralere plaats krijgt. Een 'risicojongere' is:

> *"[E]en jongere die wordt geconfronteerd met veelvoudige sociale en individuele problemen en dientengevolge het risico loopt om vroegtijdig schoolverlater, werkeloos en/of crimineel te worden" (Van der Hof et al, 2009).*

Op basis van gedeelde identiteiten van kinderen kan worden vastgesteld welke jongeren (potentieel) risicojongeren zijn. Deze ontwikkeling vormt onderdeel van het eerder aangehaalde risicodenken in de samenleving en het geloof in de maakbaarheid van onze maatschappij.

Het brede EKD wordt vooral bepleit door de vier grote steden – Amsterdam, Den Haag, Rotterdam en Utrecht – die in een brief aan de minister hebben laten weten dat zij zullen overgaan tot volledige integratie van alle beschikbare gegevens over kinderen in de verschillende contexten, omdat alleen zo de (potentiële) problemen in gezinnen optimaal kunnen worden gemonteerd. Rotterdam is bijvoorbeeld al redelijk ver in het opzetten van een breed toegankelijk EKD. Onder de naam KIDOS is het EKD daar sinds 2008 operationeel en daarin wordt vanaf de zwangerschap informatie over individuele kinderen opgeslagen. Vooralsnog is dit nog JGZ-data (inmiddels uitgebreid met informatie verzameld door verloskundigen), maar er zijn plannen om een beroep te doen op huisartsen en de kinderopvang. Bovendien zullen via het Centrum voor Jeugd en Gezin – een samenwerkingsverband van het consultatiebureau, de GGD en Bureau Jeugdzorg – ook andere JZ-professionals (onderwijs (leerlingvolgsysteem, schoolmaatschappelijk werk), jeugd-GGZ en jeugdzorg) worden toegevoegd aan het systeem om aldus een compleet beeld van kinderen te realiseren. Op termijn moet KIDOS hét centrale toegangsportaal worden voor de jeugdzorg en daarmee een instrument om kinderen gedurende een belangrijk deel van hun leven systematisch in de gaten te houden.

Hier aanbeland zou het EKD zoals voorzien door de vier grote steden niet alleen samengestelde maar zelfs gedeelde identiteiten van kinderen en jongeren omvatten. Teruggrijpend op de in het vorige hoofdstuk behandelde risico's aan de constructie en het gebruik van deze identiteiten zien we in de geraadpleegde

beleidsstukken niets terug van overwegingen die wijzen op aandacht voor de mogelijke negatieve effecten en hoe ermee om te gaan. Als er al een kritische kanttekening wordt gemaakt dan betreft deze "slechts" de bescherming van privacy en persoonsgegevens waarvan echter wordt verwacht dat ze niet in de weg zullen – of mogen – staan aan de ontwikkeling.

5.3 Conclusie

Tijdens het onderzoek bleek het lastig om praktijkvoorbeelden van samengestelde en gedeelde identiteiten te achterhalen. De meest in het ook springende ontwikkeling in dit verband is momenteel het implementeren van het EKD in de jeugdzorg, waarbij het in een aantal steden in ieder geval de bedoeling lijkt te zijn om over verschillende beleidsinstanties heen deelidentiteiten van kinderen en jongeren samen te voegen tot data sets en risicoprofielen die een uiterst gedetailleerd beeld van hen bieden. Vooralsnog bestaat er in beleidsdocumenten niet of nauwelijks aandacht voor de mogelijke risico's aan het ontstaan en gebruik van moderne identiteiten in de jeugdzorg-context, laat staan voor maatregelen om eventuele negatieve effecten het hoofd te bieden (Van der Hof e.a., 2009; Van der Hof, Keymolen, 2010). Dit kan ermee te maken hebben dat de ontwikkeling van deze identiteiten nog in de kinderschoenen staat. Dat neem niet weg dat daar waar beleidsplannen om rijke identiteiten van burgers te creëren, zoals bij het EKD, steeds vastere vorm aan beginnen te nemen een kritische houding mag worden verwacht ten aanzien van de keuzes die worden gemaakt en de betekenis daarvan voor de burger, mede in haar relatie tot de overheid. Tijdens het onderzoek is het niet gelukt om ervaringen van de burger mee te nemen in het waarderen van de ontwikkeling van enkelvoudige naar steeds complexere identiteiten, maar het zou goed zijn om deze te monitoren en te waarderen wanneer en waar moderne identiteitsconstructies hun intrede doen.

6. Conclusies

6.1 Trends en definities

In het onderzoek is geschetst hoe traditionele papieren registraties binnen de overheid mettertijd zijn vervangen door digitale identiteiten. Het concept 'digitale identiteit' wordt in de literatuur op verschillende manieren gedefinieerd. In onze studie hebben aansluiting gezocht bij het door Clarke gebruikte concept 'digital persona'. Dit omschrijft hij als volgt:

> *"A model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual."*

Bij het creëren van een 'digital persona' gaat er uitdrukkelijk om een representatief beeld van een persoon (voor een bepaald doel of in een bepaalde context) te realiseren om op basis daarvan te handelen of beslissingen te nemen over dit individu. Clarke's 'digital personae' zijn door het feit dat ze fungeren als representaties van individuen in de fysieke wereld 'volwaardige' identiteiten.

Binnen het concept 'digital persona' maakt Clarke vervolgens onderscheid tussen 'projected digital persona' en 'imposed digital persona'. 'Projected digital persona' omvat het beeld dat door het individu bewust of onbewust wordt geschapen naar de buitenwereld. De burger kan bijvoorbeeld informatie over zichzelf aanleveren bij een overheidsinstantie. Van 'imposed digital persona' is sprake wanneer het persona bestaat uit data die ontstaat door interpretatie van de houder van het persona over de betreffende burger. De overheid kan zelf informatie over burgers verzamelen zonder dat deze daarbij betrokken zijn (zuivere 'imposed persona'), maar zij kan ook op basis van door de burger aangeleverde data eigen gegevens en beoordelingen toevoegen (hybride 'imposed persona'). Een burger wordt niet gerepresenteerd door één enkele (imposed of projected) digital persona, maar kan er afhankelijk van context en doel verschillende hebben. Hier raakt het concept aan Goffman's idee van 'audience segregation': we hebben verschillende rollen afhankelijk van het te verwachten publiek. In dit geval spreken we dan ook van 'deelidentiteit' of 'digitale deelidentiteit' in een gedigitaliseerde omgeving.

Met de toenemende digitalisering van data en identiteiten evolueren eenvoudige registraties zich tot complexere datasets of digitale identiteiten die gedetailleerde overzichten over de identiteit van burgers bieden. De moderne digitale identiteiten kunnen functioneren als de representaties van mensen van vlees en bloed en kunnen de grondslag vormen voor overheidsbeslissingen zonder inbreng van de 'echte' burger. Bij enkelvoudige digitale identiteiten gaat het vooralsnog om gegevensverzamelingen zoals die door een enkele organisatie worden bijgehouden. Ook hier zien we echter al een tendens waarin op basis van steeds rijkere representaties beslissingen over individuele burgers kunnen worden

genomen die verder rijken dan waarvoor de gegevens in strikte zin oorspronkelijk waren verzameld (denk aan het voorbeeld van de kinderbijslag). Er is hier nog steeds sprake van een duidelijke band tussen doel en gebruik van de verzamelde gegevens. Op beperkte schaal is er echter ook al een ontwikkeling zichtbaar, waarbij deze band losser is en misschien wel wordt losgelaten. Het gaat dan om identiteiten die worden geconstrueerd door verschillende deelidentiteiten met elkaar te verbinden.

Als gevolg van een toenemende interconnectiviteit binnen het openbaar bestuur ontstaat door de samenvoeging van digitale deelidentiteiten wat we hebben genoemd samengestelde en gedeelde identiteiten. Samengestelde identiteiten zijn volgens ons:

> *Digitale identiteit die zijn uitgebouwd door van twee of meer onafhankelijke entiteiten afkomstige digitale deelidentiteiten samen te voegen.*

Een samengestelde identiteit wordt door één partij gebruikt (de samensteller). De samengestelde identiteit bestaat uit informatie vanuit verschillende bronnen. Gedeelde identiteiten gaan nog een stap verder doordat de digitale deelidentiteiten over verschillende beleidscontexten heen worden gecombineerd en gebruikt door meerdere partijen. In het onderzoek hebben we deze identiteiten gedefinieerd als:

> *Digitale identiteit die zijn uitgebouwd door van twee of meer onafhankelijke entiteiten afkomstige digitale deelidentiteiten samen te voegen over verschillende beleidscontexten heen en die in de verschillende constituerende domeinen wordt gebruikt.*

Het doel van deze moderne identiteitsconstructie is om complete identiteiten van burgers te creëren teneinde een beleidsdomein overstijgende aanpak van sociale problemen mogelijk te maken. Deze constructie is geen triviale operatie, omdat gegevensverzamelingen uit verschillende contexten uiteenlopend zijn vormgegeven en niet altijd eenvoudig kunnen worden gecombineerd. Unieke persoonsnummers, zoals het BurgerService Nummer, en authentieke bronnen, zoals de basisregistraties, vormen onmisbare instrumenten om deze identiteiten zo effectief en efficiënt mogelijk te creëren en gebruiken.

Voor de overheid zijn samengestelde en gedeelde identiteiten belangrijk om het hoofd te kunnen bieden aan ingewikkelde beleidsvraagstukken waarvoor ze zich gesteld ziet in een steeds complexer wordende samenleving. In toenemende mate wordt er geageerd vanuit sociaal onwenselijk geachte situaties ongeacht of daar diverse beleidsdomeinen en instanties bij betrokken zijn. Soms is juist de wens om verschillende partijen onderling werkzaamheden zo goed mogelijk af te laten stemmen aangegrepen om gedeelde identiteiten te creëren. Deze ontwikkeling zien we nu plaatsvinden bij het Elektronisch Kind Dossier, zoals beschreven in hoofdstuk 5. Overigens bleek het tijdens het empirisch deel van het onderzoek lastig om verder al voorbeelden van deze moderne identiteitsconstructies te vinden. Wellicht is de reden dat we hier nog aan het begin van een ontwikkeling staan.

Daarnaast is overheidsbeleid meer en meer gericht op het inschatten en voorkomen van maatschappelijke risico's, waardoor de behoefte aan context-overschrijdende digitale data en identiteiten groeit. Risicoprofilering is een voorbeeld van een relevante ontwikkeling in dit verband. Samengestelde en gedeelde identiteiten bieden onmiskenbaar kansen voor moderne beleidsvorming en -oplossingen, maar er zijn ook schaduwkanten.

6.2 Risico's

In ons onderzoek hebben we op basis van de literatuur een inventarisatie gemaakt van (potentiële) risico's voor de constructie en met het name het gebruik van moderne digitale identiteiten, zoals samengestelde en gedeelde identiteiten. We hebben daarbij een onderscheid gemaakt tussen fundamentele en praktische risico's.

Fundamentele risico's:

Ondermijning van mogelijkheden tot contextscheiding – Als identiteitsinformatie uit meerdere contexten wordt samengevoegd zonder dat rekenschap wordt gegeven van uiteenlopende regels, waarden en gebruiken binnen de afzonderlijke contexten wordt de burger mogelijkheden ontnomen om hun representatie of rol af te stemmen op die afzonderlijke contexten. Meer informatie betekent niet per definitie betere besluiten en informatie die niet relevant is kan besluiten onredelijk beïnvloeden;

Decontextualisering – Bij het contextoverschrijdend combineren van deelidentiteiten kan context-informatie die relevant is om de identiteiten correct te interpreteren wegvallen of de ontstane gedeelde identiteiten vormen een inconsistente of onjuiste representatie van de betrokken burger. Relevant is in dit verband het door Nissenbaum geïntroduceerde concept 'contextual integrity' waarmee zij onder meer aangeeft dat het, mede gelet op (wettelijke) taken en doelen, per context sterk kan verschillen welke informatie passend of noodzakelijk is om uit te wisselen. Volgens Nissenbaum dienen veranderingen in bestaande praktijken zorgvuldig te worden onderbouwd in het licht van individuele rechten en vrijheden van burgers.

Vermindering van autonomie en verlies van controle – In moderne systemen van identiteitsconstructie worden identiteiten van burgers in toenemende mate voor hen in plaats van – mede – door hen geconstrueerd op basis van de steeds uitgebreidere data-set die de overheid van hen heeft. Deze identiteiten kunnen buiten het zicht van de burger een eigen leven gaan leiden binnen de overheidsbureaucratie. Burgers zijn dan niet alleen niet betrokken bij of

geïnformeerd over de keuzes over wat hun identiteit wel of niet behelst, maar verliezen bovendien de controle over hoe hun identiteiten worden gebruikt.

Ondermijning van mogelijkheden tot 'identity negotiation' – Periodieke verificatie van de inhoud van identiteiten ('identity negotiation') is belangrijk om deze actueel te houden. Op het moment dat identiteiten een eigen leven gaan leiden binnen de overheidsadministratie zonder dat op gestelde momenten rekenschap wordt gegeven van de correctheid van digitale representaties van burgers door terugkoppeling met hen, is er een gerede kans op onverwachte of foutieve beslissingen met mogelijke vergaande consequenties voor betrokkenen.

Stereotypering – Vanuit het oogpunt van beleidsvorming en -uitvoering is het noodzakelijk dat burgers worden 'gevangen' in categorieën waarop dat beleid zich kan richten. Stereotypering kan echter ook leiden tot ongerechtvaardigde vooroordelen ten aanzien van en onredelijke of ongewilde uitsluiting van burgers. Een goede beoordeling in concrete situaties vereist dat de mens achter de digitale representatie zichtbaar blijft.

Faciliteren van identiteitsfraude – Digitaliseringsprocessen brengen relatief nieuwe kwetsbaarheden met zich mee, zoals identiteitsfraude of identiteitsdiefstal, in welk geval derden persoonlijke gegevens of identiteiten misbruiken voor persoonlijk gewin. Unieke persoonsnummers spelen een belangrijke rol in het construeren van samengestelde en gedeelde digitale identiteiten maar kunnen tevens faciliteren in het plegen van identiteitsfraude.

Praktische risico's:

Fouten door koppeling – Koppeling van deelidentiteiten vergroot de kans op fouten doordat in het op elkaar aansluiten van technisch-organisatorische processen op verschillende niveaus dingen mis kunnen gaan. Bovendien kan een toegenomen data-intensiteit een omgekeerd evenredig effect hebben op de datakwaliteit. Kleine fouten die doorwerken in de keten kunnen uiteindelijk vergaande consequenties hebben. Voor de burger is dan vaak onduidelijk wie verantwoordelijk is voor fouten.

Intransparante fouten – Rijkere identiteiten maken de burger steeds transparanter voor de overheid, maar op een wijze die door de complexiteit van informatiseringsprocessen intransparant is voor de burger. Dit kan leiden tot situaties waarin fouten die ontstaan evenmin transparant zijn voor de burger. Het kan onduidelijk zijn dat er iets is misgegaan in zijn "dossier". Opnieuw kan het voor de burger lastig zijn om te ageren wanneer ook onduidelijk is waar de fout is ontstaan en welke instantie verantwoordelijkheid draagt.

Deze (potentiële) risico's vereisen wat ons betreft dat nieuwe vormen van identiteitsconstructie met de grootst mogelijke zorgvuldigheid worden betracht.

De overheid zal nauwgezet moeten onderzoeken in hoeverre (potentiële) negatieve externaliteiten van veranderingen in de identiteitsconstructie en meer algemeen het persoonsinformatiebeleid kunnen worden vermeden en welke maatregelen noodzakelijk zijn om eventuele ongewenste effecten te verwijderen en recht te zetten.

6.3 Slotoverwegingen

Eerder gaven we aan dat we nog aan het begin staan van een ontwikkeling naar samengestelde en gedeelde identiteiten. Daardoor was het helaas niet mogelijk om nu al iets te zeggen over de effecten van de constructie en het gebruik van deze identiteiten en de ervaringen van burgers daaromtrent. Tegelijkertijd biedt het de kans om tijdig te wijzen op potentiële risico's (zie vorige paragraaf) en verdere overwegingen mee te geven voor toekomstig identiteits- en persoonsinformatiebeleid.

De ontwikkelingen zoals in deze rapportage besproken hebben de neiging om een eigen dynamiek te ontwikkelingen. Is eenmaal een richting gekozen dan is het lastig, zo niet onmogelijk, om nog een andere kant op te gaan of de route te verleggen. Eenmaal gemaakte keuzes werken door in het systeem en kunnen verregaande consequenties hebben voor de relatie burger – overheid. Alvorens definitieve beslissingen te nemen over identiteitsconstructie en verrijking van identiteiten is het daarom goed om heel zorgvuldig verschillende opties en hun gevolgen tegen elkaar af te wegen. Zorgvuldigheid is belangrijker dan snelheid. Zo kun je je afvragen of meer informatie en dus rijkere identiteiten wel altijd tot betere overheidsbeslissingen leiden. Tenslotte kan de kans op fouten toenemen als datakwaliteit onvoldoende wordt gegarandeerd.

In meer fundamentele zin kun je je de vraag stellen of steeds rijkere identiteiten noodzakelijk zijn. In het geval van het Elektronisch Kind Dossier wordt wel gezegd dat het weinig uithaalt, omdat probleem– of risicojongeren vaak al wel bekend zijn bij de aangewezen instanties. Om het daadwerkelijke probleem – betere afstemming van werk tussen deze instanties – op te lossen bestaan andere middelen die minder vergaande consequenties hebben voor de kinderen en jongeren. Hier is eveneens relevant het beginsel van selectiviteit ('select before you collect'). Bedenk goed welke deelidentiteiten of identiteitsinformatie echt noodzakelijk is in plaats van automatisch *alle* mogelijke data te verzamelen.

Uitgangspunt zou wat ons betreft moeten zijn dat het voor burger transparant is wat er met hun identiteiten gebeurt binnen de overheidsadministratie. Wellicht zou er kunnen worden nagedacht over modellen waarin de burger meer controle houdt over zijn deelidentiteiten en het gebruik ervan door de overheid (en daarbuiten). Op die manier wordt voorkomen dat digitale identiteiten te ver abstraheren van de persoon van vlees en bloed die ze representeren. Burgers kunnen fouten constateren en deze bij de verantwoordelijke instanties melden. Dat laatste betekent dat er naast systeem– en datatransparantie ook sprake moet zijn van organisatorische transparantie en een heldere verdeling van verantwoordelijkheden.

Bibliografie

Anderson, Ross, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse (2009) Database State, Place.

Baumeister, Roy F. (1986a) Identity: cultural change and the struggle for self. New York: Oxford University Press.

Baumeister, Roy F. (1986b) Public self and private self. New York: Springer-Verlag.

boyd, danah (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. in: David Buckingham (ed.), MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume Cambridge, MA: MIT Press.

Castells, Manuel (1996) The rise of the network society. Cambridge, Mass.: Blackwell Publishers.

Castells, Manuel (1997) The power of identity. Malden, Mass.: Blackwell.

Castells, Manuel (1998) End of millennium. Malden, MA: Blackwell Publishers.

Clarke, R. (1994) The Digital Persona and Its Application to Data Surveillance, The information society, 10, 77-92.

Clarke, R. (2003) Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper. in: 16th Bled eCommerce Conference: eTransformation. Bled, Slovenia.

Cooley, Charles Horton (1922) Human nature and the social order. New York ; Chicago: C. Scribner's sons.

Cooper, Robbie (2007) Alter Ego: Avatars and their Creators: Chris Boot.

Donath, J. and d boyd (2004) Public displays of connection, BT Technology Journal, 22, 4, 71-82.

Gandy, Oscar H. (1993) The panoptic sort : a political economy of personal information. Boulder, Colo.: Westview.

Garland, D. (2001) The Culture of Control, Crime and Social Order in Contemporary Society. Oxford: Oxford University Press.

Gergen, Kenneth J. (1991) The saturated self: dilemmas of identity in contemporary life. [New York]: Basic Books.

Gergen, Kenneth J. (2009) An invitation to social construction, 2nd edition. Thousand Oaks, CA: SAGE Publications Ltd.

Giddens, A. (1999) Risk and Responsibility, The Modern Law Review, 62, 1, 1-10.

Giddens, Anthony (1991) Modernity and self-identity: self and society in the late modern age. Stanford, Calif.: Stanford University Press.

Goffman, E. (1956) The presentation of self in everyday life. Edinburgh: University of Edinburgh.

Grijpink, J. (2006) Indentiteitsfraude en overheid, Justitiële verkenningen, 7/06, nr. 32, 37-57.

Grijpink, J. (2007) Keteninformatisering, met toepassing op de justitiële bedrijfsketen. Den Haag: Sdu Uitgevers.

Hansen, Marit and Andreas Pfitzmann (2008) Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology, working document, Place.

Heemskerk, P. e.a. (2001) Meer doen met minder gegevens. Een onderzoek naar een stelsel rond

Authentieke registraties (Concept rapport 28-6-2001), Place.

Hildebrandt, Mireille , Bert-Jaap Koops Koops and Katja de Vries (2008) FIDIS D7.14a: Where Idem-Identity meets Ipse-Identity. Conceptual Explorations, Place.

van der Hof, S. , R.E. Leenes and S. Fennell (2009) Framing Citizen's Identities, The construction of personal identities in new modes of government in the Netherlands, Research on Personal identification and identity management in new modes of government, Place.

van der Hof, S., S. Fennell-van Esch, A.P.C Roosendaal and M.B. Voulon (2008) Wettelijk kader e-Overheid: Juridische eisen ten aanzien van de e-Overheid en ten aanzien van een interoperabiliteitsraamwerk, Place.

Hof, S. van der, S. Fennell-van Esch, A.P.C Roosendaal and M.B. Voulon (2008) Wettelijk kader e-Overheid: Juridische eisen ten aanzien van de e-Overheid en ten aanzien van een interoperabiliteitsraamwerk, Place.

van der Hof, Simone and Esther Keymolen (2010) Shaping Minors with Major Shifts, Electronic Child Records in the Netherlands, Information Polity, forthcoming.

ICCP. and SNG. (2003) Identity Management Systems (IMS): Identification and Comparison Study, Place.

Introna, Lucas (1997) Privacy and the Computer: Why We Need Privacy in the Information Society, Metaphilosophy, 28, 3, 259–75.

James, William (1890) The principles of psychology. New York,: H. Holt and company.

de Jong, Jorrit , Arre Zuurmond, Joeri van den Steenhoven and Lobke van der Meulen (2008) Kafka in de polder – Handboek voor opsporen en oplossen van overbodige bureaucratie. Den Haag: SDU Uitgevers.

Keymolen, E.L.O. (2007) Onzichtbare Zichtbaarheid. Helmuth Plessner ontmoet profiling, Place.

Koops, B-J., Ronald Leenes, Martin Meints, Nicole van der Meulen and David-Olivier Jacquet-Chiffelle (2008) A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues, Information Communication & Society.

Lyon, David (2001) Surveillance society : monitoring everyday life. Buckingham [England] ; Phildelphia: Open University Press.

Lyon, David (2004) Globalizing Surevillance; Comparative and Sociological Perspectives, International Sociology, 19, 2, 135-49.

Mead, George Herbert and Charles W. Morris (1934) Mind, self & society from the standpoint of a social behaviorist. Chicago, Ill.,: The University of Chicago press.

Nissenbaum, Helen (2004) Privacy as Contextual Integrity, Washington Law Review, 79, 1, 119-58, http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

Ombudsman, Nationale (2009) De burger in de ketens, Verslag van de Nationale Ombudsman over 2008, Place.

Prins, J.E.J. (2009) Heeft digitale jeugdzorg de toekomst? in: M. van den Berg (ed.), In de greep van de technologie, Nieuwe toepassingen en het gedrag van de burger. Amsterdam: Van Gennip, 23-50.

Prins, J.E.J. and N.S. van der Meulen (2006) indentiteitsdiefstal: lessen uit het buitenland, Justitiële verkenningen, 7/06, nr. 32, 8-22.

Projectgroep Visie op de politiefunctie (2005) Politie in ontwikkeling. Visie op de politiefunctie, Place.

Raab, C. (2009) Identity: Difference and Categorization. in: Ian Kerr, Valerie Steeves and Carole Lucock (eds.), Lessons from the Identity Trail: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 227-44.

Rachels, J. (1975) Why privacy is important, Philosophy and Public Affairs, 323-33.

Ricoeur, P. (1990 (1992)) Oneself as Another (Soi-même comme un autre), trans. Kathleen Blamey. Chicago: University of Chicago Press.

Ringeling, Arthur (2001) Rare klanten hoor, die klanten van de overheid. in: van Hendricus Petrus Maria Duivenboden and Miriam Lips (eds.), Klantgericht werken in de publieke sector

Inrichting van de elektronische overheid. Utrecht: Uitgeverij LEMMA BV, 33-48.

Robinson, Laura (2007) The cyberself: the self-ing project goes online, symbolic interaction in the digital age, New Media & Society, 9, 1, 93-110.

Schauer, F. (2003) Profiles, probabilities and Stereotypes. Cambridge: Mass.: Harvard University Press.

Schermer, Bart W. and Ton Wagemans (2009) Onze digitale schaduw: Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat, Place.

Smith, Robert Ellis (2004) Ben Franklin's Web Site: Privacy and Curiosity From Plymouth Rock to the Internet: Sheridan Books.

Solove, Daniel J. (2007a) 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy: SSRN.

Solove, Daniel J. (2007b) The future of reputation; Gossip, Rumor, and Privcay on the Internet: Yale University Press.

Swann, W.B. (2005) The self and identity negotiation, Interaction Studies, 6, 1, 69-83.

Turkle, S. (1997) Life on Screen. London: Phoenix.

Vedder, A.H., L. van der Wees, B.J. Koops and P.J.A.(2007). De Hert (2007) Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw, Place.

W., Lyon David (2001) Surveillance Society; Monitoring everyday life: Open University Press.

Zarsky, Tal Z. (2002) Mine your own business!: Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion., Yale Journal of Law & Technology, 5, 4, 17-47.

Zarsky, Tal Z. (2004) Desperately Seeking Solutions: Using Implementation-based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society Maine Law Review, 56, 14-59.

Bijlagen

Vragenlijst 'Gedeelde identiteiten'

Introductie

Steeds meer overheidsdiensten zijn via elektronische weg beschikbaar voor de burger. Veel burgers doen hun belastingaangifte via Internet, of vragen online uittreksels uit het bevolkingsregister op of dienen per mail een vergunningaanvraag in. Elektronische dienstverlening leidt tot elektronische dossiers over de gebruikers van deze diensten. Deze dossiers worden steeds vaker gekoppeld. Op die manier kan de dienstverlening worden verbeterd (eenmalige gegevensverstrekking, personalisatie), kan een effectievere samenwerking tussen verschillende organisaties (bijvoorbeeld in het kader van de jeugdzorg) worden gerealiseerd en kan fraude worden opgespoord. Tegelijkertijd brengen dergelijke koppelingen ook risico's met zich mee. De overheid krijgt bijvoorbeeld een steeds completer beeld van de burger. Hierdoor voelen we ons misschien niet meer onbevangen is ons doen en laten. Maar ook kan het koppelen van gegevens leiden tot een onjuist beeld van een bepaalde burger. Ook kan het zijn dat burgers moeilijk afkomen van eenmaal in het systeem opgeslagen negatieve kwalificaties (bijvoorbeeld fraudeur, slechte ouder, risicojongere). Dit alles kan tot ongewenste individuele en sociale consequenties leiden.

Het doel van dit onderzoek is de effecten van bestandskoppelingen van overheidsinstanties in kaart te brengen aan de hand van concrete ervaringen van burgers.

We beginnen met een aantal algemene vragen.

1. Hoe vaak gebruikt u elektronische overheidsdiensten?
    1. zelden (ongeveer 1 maal per jaar)
    2. soms (2 – 4 maal per jaar)
    3. regelmatig (5 – 10 maal per jaar)
2. Welke elektronische overheidsdiensten gebruikt u?
    1. open vraag met 4 antwoordvakken
3. In het algemeen gesproken, zou u dan zeggen:
    1. dat de meeste mensen te vertrouwen zijn
    2. dat je niet voorzichtig genoeg kunt zijn in de omgang met mensen
4. Denkt u dat de meeste mensen misbruik van u zouden maken als ze daar de kans voor krijgen, of dat zij meestal eerlijk handelen?
    1. ze zouden misbruik van me maken
    2. ze handelen meestal eerlijk
5. Hoeveel vertrouwen heeft u in het algemeen dat onderstaande organisaties in de publieke sector zorgvuldig met u, uw belang en uw persoonlijke gegevens omgaan?
    1. De gemeente (1 = helemaal niet, 2 = nauwelijks, 3 = neutraal, 4 = redelijk wat, 5 = veel)

2. De rijksoverheid
3. De belastingdienst

We gaan nu in op de concrete aanleiding waarom u aan ons onderzoek meedoet. U heeft een concrete ervaring met (elektronische) dienstverlening met een overheidsinstantie die een voor u 'verassende' ervaring heeft opgeleverd (hierna het voorval). Roept u deze ervaring in herinnering.

6. Wat voor soort contact betrof het voorval?
    1. baliecontact
    2. online contact (via website of email)
    3. schriftelijk contact (via brief of formulier)
7. Met welke overheidsinstantie was u in contact?
    1. open vraag
8. Met welk doel trad u met deze instantie in contact?
    1. Ik kreeg een aanslag (bijvoorbeeld belastingaanslag)
    2. Ik wilde iets aanvragen (bijvoorbeeld een subsidie of document)
    3. Ik werd gevraagd bepaalde gegevens aan te leveren/bij te werken
    4. Ik wilde mijn mening geven/een klacht uiten
9. Wat verbaasde u aan het resultaat/voorval (bijvoorbeeld de beslissing)?
    1. er is andere informatie gebruikt dan ik heb opgegeven
    2. er is onjuiste informatie gebruikt
    3. er is informatie gebruikt die ik niet heb opgegeven
    4. ik heb iets gekregen waarom ik niet heb gevraagd
    5. anders, namelijk …
10. Waardoor komt dit volgens u?
    1. Er zijn bestanden aan elkaar gekoppeld
    2. er zijn gegevens aan elkaar gekoppeld die uit hun verband zijn gehaald
        1. toelichting…
    3. Er is informatie over/van iemand anders gebruikt (persoonsverwisseling)
    4. Er is een fout gemaakt in de verwerking van gegevens
    5. anders, namelijk …
11. Welke effect(en) heeft dit voorval voor u? (meerdere opties mogelijk)
    1. er bestaat nu een negatief beeld over mij bij de betreffende instantie
    2. ze denken dat ik een fraudeur ben
    3. ik heb iets **niet** gekregen waar ik (volgens mij) wel recht op heb
    4. ik heb iets gekregen waar ik (volgens mij) geen recht op heb
    5. anders, namelijk …

12. Wat heeft u ondernomen als gevolg van het voorval?
    1. ik heb (veel) moeite gehad de situatie recht te zetten
    2. ik heb het laten zitten
    3. ik hoefde niets te doen, de instantie kwam zelf achter de fout
    4. anders, namelijk …
13. Is uw vertrouwen in de overheid als gevolg van dit voorval
    1. toegenomen
    2. gelijk gebleven
    3. afgenomen

Afsluiting.

14. Wat is uw geslacht?
15. Wat is uw leeftijd?
16. Wat is uw etnische achtergrond?
    1. Nederlands
    2. Surinaams
    3. Antilliaans
    4. Turks
    5. Marokkaans
    6. anders…
17. [als niet NL] Zou dit een rol gespeeld kunnen hebben in het voorval, bijvoorbeeld omdat u niet goed begreep wat er van u verwacht werd?
    1. ja, nee + toelichting
18. Heeft u opmerkingen of suggesties voor de onderzoekers?
19. Mogen we contact met u opnemen om uitvoeriger van u te horen over het voorval?
    1. ja, neem contact met mij op via email:
    2. ja, bel mij op:

Alle door u verstrekte informatie wordt vertrouwelijk behandeld en alleen voor wetenschappelijke doeleinden gebruikt.

Hartelijk dank voor uw medewerking!

1. Wat is uw geslacht?
2. Wat is uw leeftijd?
3. Wat is uw nationaliteit?

4. Hoe regelmatig gebruikt u elektronische overheidsdiensten?
5. Van welke elektronische overheidsdiensten maakt u gebruik?
6. Hoe groot is uw vertrouwen in de overheid op een schaal van 1-10?
7. Heeft het gebruik van elektronische overheidsdiensten geleid tot (onverwachte) positieve effecten? Zo ja welke? Zo nee, ga door naar vraag [...]
8. Welke consequenties hadden de positieve effecten voor u persoonlijk?
9. Hebben uw ervaringen ertoe geleid dat u meer vertrouwen heeft in de elektronische overheid?
10. Hebben uw ervaringen ertoe geleid dat u meer vertrouwen heeft in de overheid?
11. Heeft het gebruik van elektronische overheidsdiensten geleid tot (onverwachte) negatieve effecten? Zo ja welke? Zo nee, ga door naar vraag [...]
12. Welke consequenties hadden de negatieve effecten voor u persoonlijk?
13. Heeft u actie ondernomen tegen de negatieve effecten? Zo ja, welke? Zo nee, ga door naar [...]
14. Wat was het resultaat van uw actie bedoeld onder 10.?
15. Hebben uw ervaringen ertoe geleid dat u minder vertrouwen heeft in de elektronische overheid? Hebben uw ervaringen ertoe geleid dat u minder vertrouwen heeft in de elektronische overheid?
16. Hebben uw ervaringen ertoe geleid dat u minder vertrouwen heeft in de overheid?
17. Hoe groot is uw vertrouwen in de overheid op een schaal van 1-10?
18. Heeft het gebruik van niet-elektronische overheidsdiensten geleid tot (onverwachte) positieve effecten? Zo ja welke? Zo nee, ga door naar vraag [...]
19. Welke consequenties hadden de positieve effecten voor u persoonlijk?
20. Hebben uw ervaringen ertoe geleid dat u meer vertrouwen heeft in de elektronische overheid?
21. Heeft het gebruik van niet-elektronische overheidsdiensten geleid tot (onverwachte) negatieve effecten? Zo ja welke? Zo nee, ga door naar vraag [...]
22. Welke consequenties hadden de negatieve effecten voor u persoonlijk?
23. Hebben uw ervaringen ertoe geleid dat u minder vertrouwen heeft in de overheid?
24. Heeft u actie ondernomen tegen de negatieve effecten? Zo ja, welke? Zo nee, ga door naar vraag [...]
25. Wat was het resultaat van uw actie bedoeld onder 10.?
26. Heeft u nog opmerkingen of suggesties?

Indien u bereid bent tot eventuele verdere toelichting aan de onderzoekers en/of op de hoogte wilt worden gehouden van de resultaten van het onderzoek dan kunt u hier uw e-mail adres invullen: [.....]

Alle door u verstrekte informatie wordt vertrouwelijk behandeld en alleen voor wetenschappelijke doeleinden gebruikt.

Hartelijk dank voor uw medewerking!